New Modes of Encryption - A Perspective and a Proposal

Virgil D. Gligor* **Pompiliu Donescu**

VDG Inc
6009 Brookside Drive
Chevy Chase, Maryland 20815

{gligor, pompiliu}@eng.umd.edu

NIST Modes of Operation Workshop
Baltimore, Maryland
October 20, 2000

(*) Part of this work was performed while on sabbatical leave from the University of Maryland, Department of Electrical and Computer Engineering, College Park, Maryland 20742

Outline

1. Security Claims

2. Operational Claims

3. Evidence

4. Examples: XCBC, XECB-MAC and PM-XOR

5. Proposal: Three* Distinct Mode Candidates

6. Intellectual Property Status

1. Security Claims for Modes of Encryption

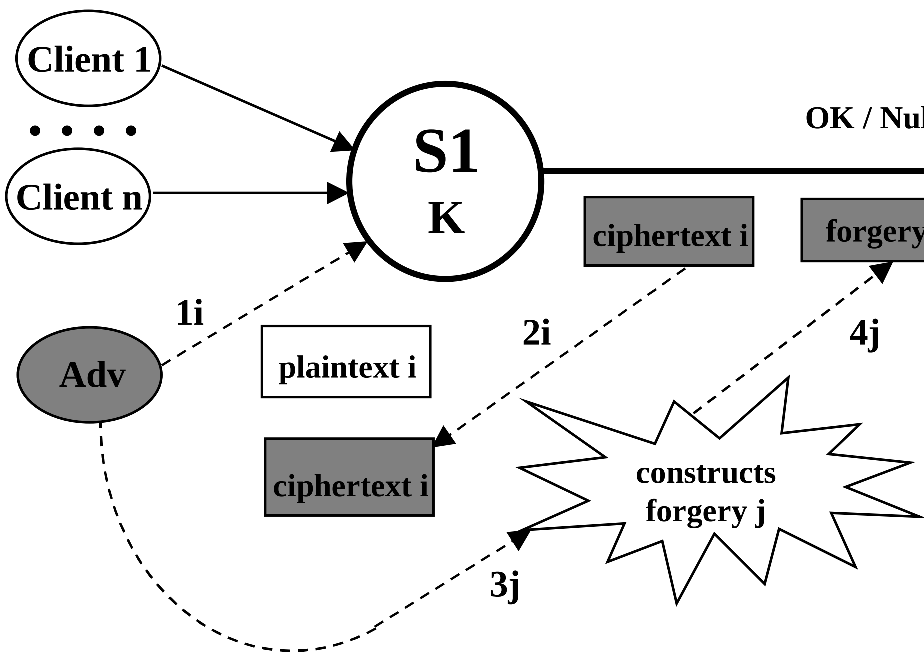
1. ***Claim*** = a security notion supported by a mode or scheme of encryption
2. Security ***Notion*** = < security goal, attack characteristics>

3. Security ***Goal***: confidentiality, integrity (authenticity), common
   - Examples:
     - confidentiality: indistinguishability (IND)
     - integrity: resistance to existential forgery (EF)
     - common: resistance to key searches (KS)
     - combinations

4. ***Attack Characteristics*** (models)
   - Examples:
     - Chosen (Known) Plaintext
     - Ciphertext-only
     - Chosen ciphertext
     - combinations

Example of a Chosen-Plaintext Attack

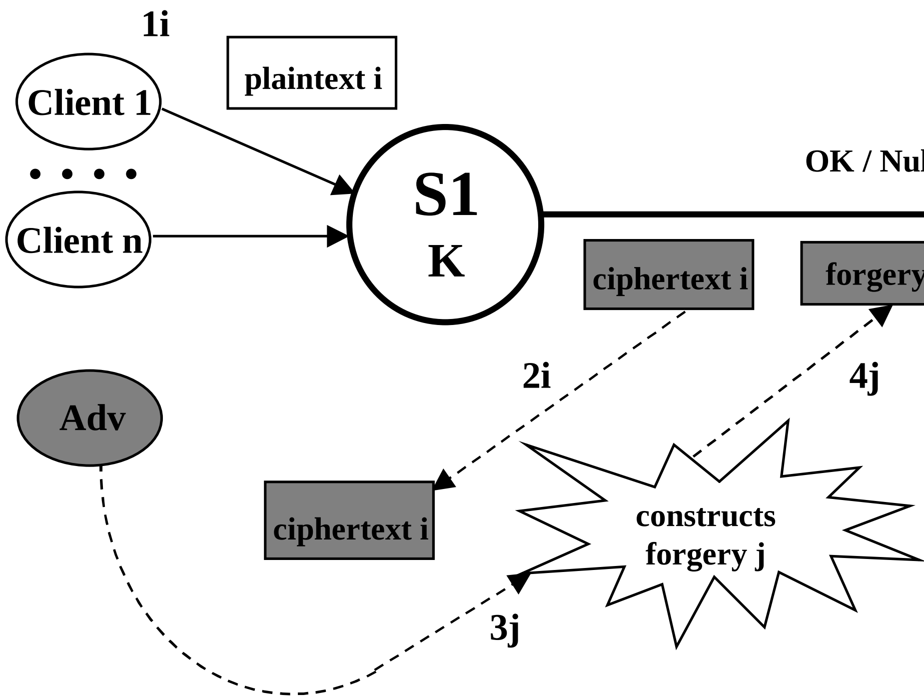
Distributed Service: S (S1, S2), shared key K; Clients: Client 1. … Adv, …, Client n
Adversary: Adv



In attack scenario:
S1 becomes an Encryption Oracle
S2 becomes a Decryption Oracle

Example of Ciphertext-only Attack

Distributed Service: S (S1, S2), shared key K; Clients: Client 1,…, Client n
Adversary: Adv is not a client



In attack scenario:
No Encryption Oracle: plaintext i is r.u.d
(Adv known absolutely nothing about plaintext i)
S2 becomes a Decryption Oracle

Example of Integrity Goals

Existential Forgery **protection (EF) : Pr[D_K(forgery) =/= Null] is negligible**

Other Integrity Notions: constraints on D_K(forgery) =/= Null

Examples:

Non-malleability **(NM) :**
given ciphertext challenge y whose plaintext x may be unknown, find forgery of the same length as y :
Pr [D_K(forgery) =/= Null and Relationship(D_K(forgery), x)] is negligible

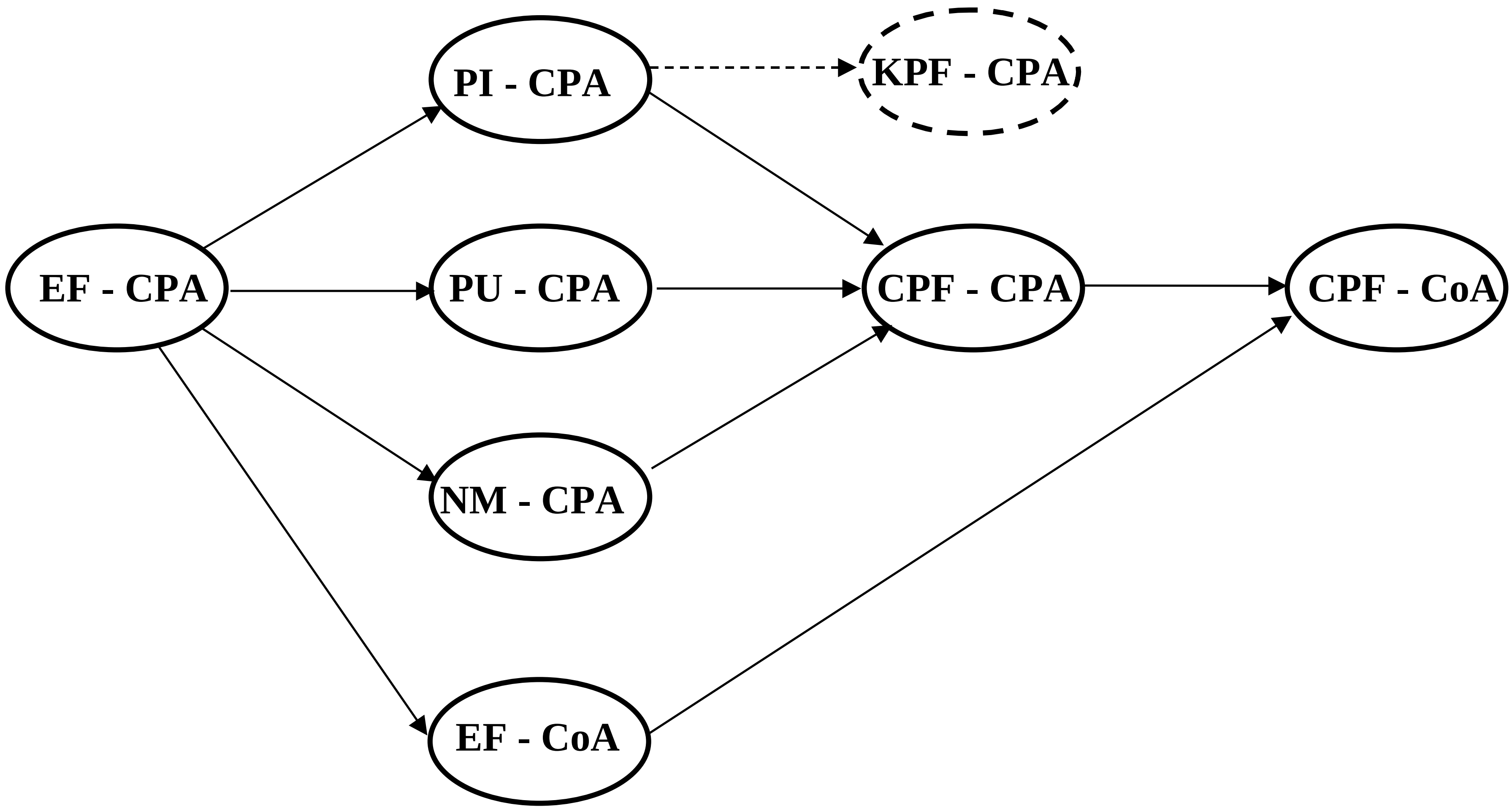
Integrity of Plaintexts **(PI) :**
Pr [D_K(forgery) =/= Null and D_K(forgery) =/= plaintexts encrypted before] is negligible

Assurance of *Plaintext Uncertainty* (PU) :
Pr [D_K(forgery) =/= Null => D_K(forgery) =/= plaintexts encrypted before and *is unknown*] is close to 1

Protection against *Chosen-Plaintext Forgery* (CPF) : given a chosen plaintext challenge *x*,
Pr [D_K(forgery) =/= Null and D_K(forgery) = *x* =/= plaintexts encrypted before] is negligible

Note: **some constraints may be integrity counter-intuitive; e.g.,**
assurance of *Known-Plaintext Forgery* (KPF)
Pr [D_K(forgery) =/= Null => D_K(forgery) is *known*] is close to 1.

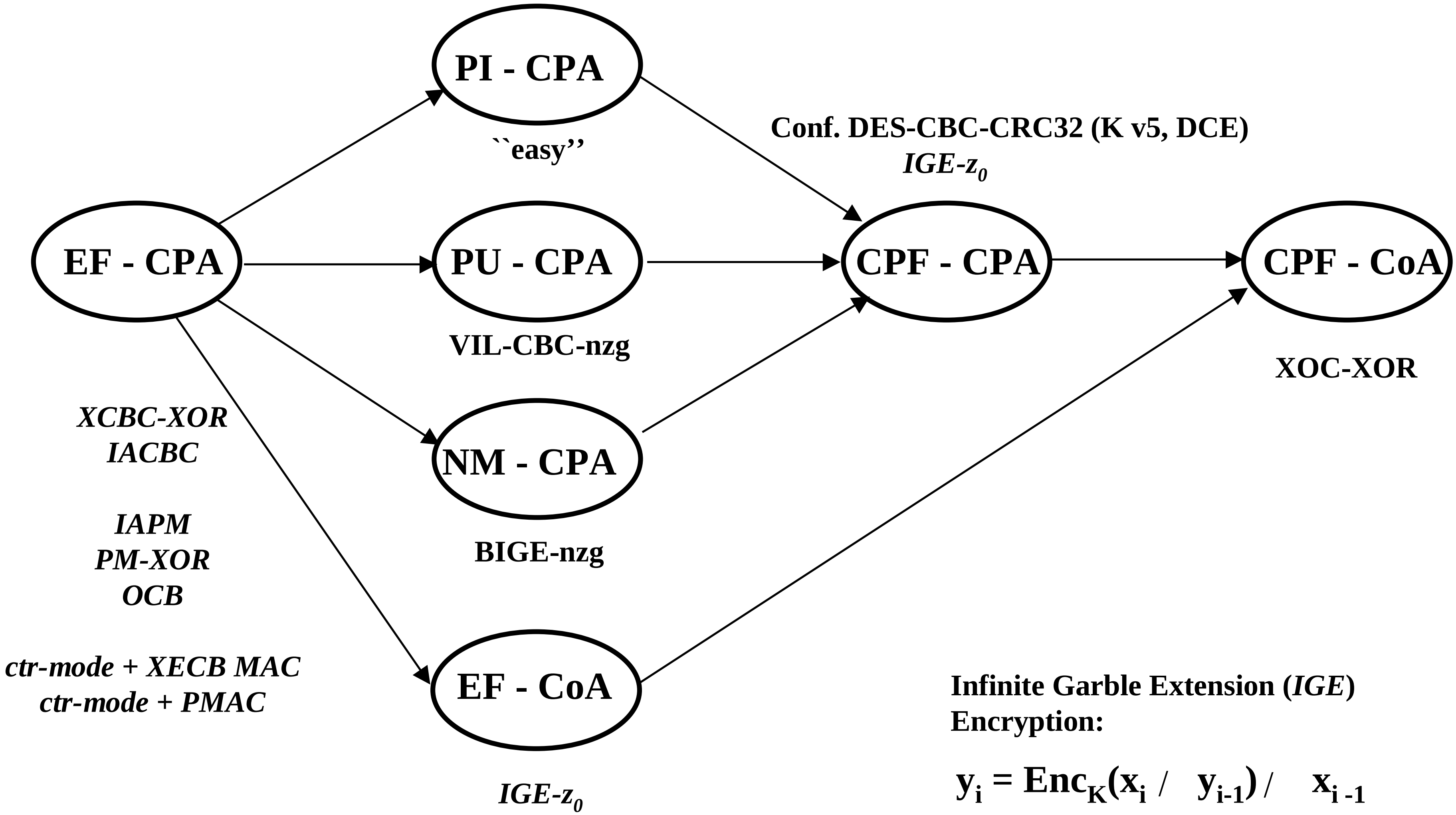
Relationships among Integrity Notions



Legend: A ⟶ B iff A ==> B and B =/=> A (``dominance'')
A ==> B iff mode is secure in A is also secure in B
B =/=> A iff mode is secure in B is not secure in A

Examples of Modes Satisfying Different Integrity Notions

Encryption Mode - "redundancy" function *or* Encryption Mode + MAC Mode



Infinite Garble Extension (*IGE*) Encryption:

$$y_i = Enc_K(x_i \;/\; y_{i-1}) \;/\; x_{i-1}$$

Note: italics designate modes presented in NIST Workshop on AES Modes of Encryption

2. Operational Claims for Modes of Encryption

1. ***Claim*** = a operational notion supported by a mode or scheme of encryption
2. Operational ***Notion*** = < operational goals, mode characteristics >
3. Operational ***Goal***: cost-performance, simplicity, others
   - Examples of (related) goals:
     - cost-performance:
       - low power consumption
       - high speed (e.g., throughput)
       - low implementation cost (e.g., hardware ``real-estate'')
     - simplicity
       - single cryptographic primitive, key
4. ***Mode Characteristics***
   - Examples:
     - State: stateless, stateful
     - Degree of parallelism
       - sequential
       - interleaved (apriori known or negotiated no. of proc. units)
       - fully parallel (independent of no. of processing units)
     - Separated Confidentiality and Integrity keys
     - Other: incremental, out-of-order processing

Examples of Operational Claims

Low- and High-End Goals

• cost-performance:	
• low power consumption	
• speed: moderate (e.g., < 100 MBS)	> 100 GBS
• low implementation cost	hardware
• simplicity	
• single cryptographic primitive (AES), key	single crypto prim.

Low- and High-End Mode Characteristics

• State: stateful	stateful, stateless
• Degree of parallelism	
• sequential (single processor)	fully parallel for Conf. & Integrity
• Separated Confidentiality and Integrity keys: No	Yes
• Others: incremental, out-of-order processing: No	Yes for both Conf. & Integrity

3. Evidence for Claims

1. Mode specification

2. Security Claim
- **goal - attack pair(s)**

3. "Proof "
- **formal: Mode spec. satisfies Security Claim**
  - **standing assumption: AES is secure w.r.t. all known attacks**
- **peer review**
- **other empirical evidence: known attacks**

4. Operational Claim
- **goal - mode characteristics pair(s)**

5. Operational evidence
- **implementation + performance tests**
- **other empirical evidence**

XCBC Encryption

Fact: Encryption is not intended to provide integrity

Motivation

- **Encryption w/o integrity checking is all but useless [Bellovin 98]**

- **Define family of encryption modes to help provide integrity with non-cryptographic "redundancy" functions**

- **Security claims: IND-CPA confidentiality and EF-CPA integrity, reasonable bounds**

- **Operational claims: preferred for Low- to Mid-End op. environment**

- **Knowledge of operational environments:**
    - **apriori obtained**
    - **discovered via negotiation**

Operational Claims

Preferred environments : low- to mid-end

Goals

- cost performance

- low power consumption
- speed: moderate to high (e.g., close to CBC-UMAC-MMX30)
- low implementation cost

- **simplicity**

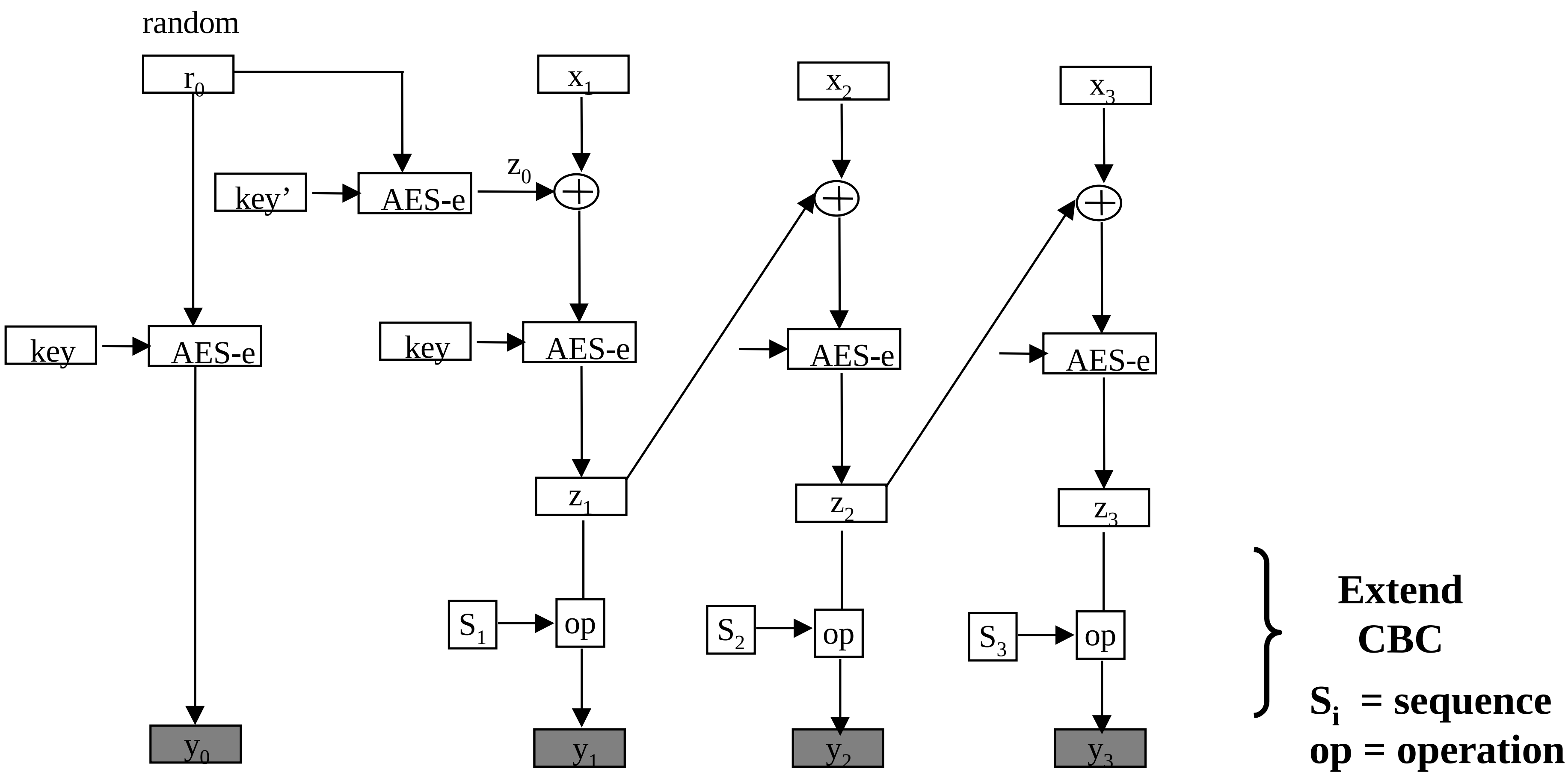
- single cryptographic primitive (AES), key

Mode Characteristics

- State: stateful, stateless
- Degree of parallelism: sequential (single processor), interleaved (known no. procs.)
- Separated Confidentiality and Integrity keys: No
- Others: incremental, out-of-order processing: Yes (if interleaved)

Stateless XCBC Scheme - Encryption of $x = x_1x_2x_3$

(single key is also possible)

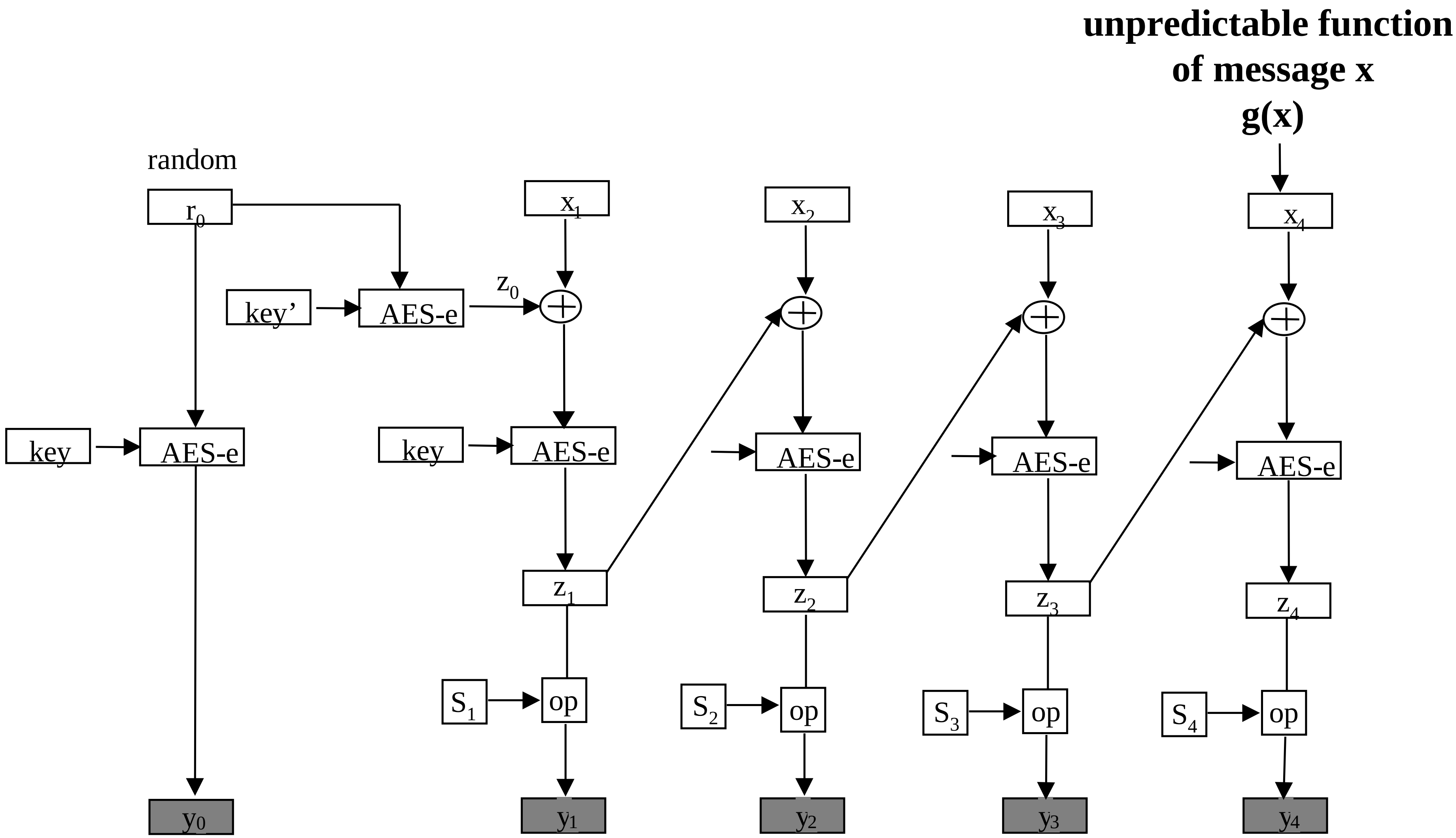


Examples of S_i and *op* combinations (+ is mod 2^l; $\oplus$ is bitwise exclusive-or)

op = + $S_i = S_{i-1} + r_0$, $S_0 = 0$ **(written as $S_i = i \times r_0$)**

Other S_i and *op* definitions exist (e.g., C.S. Jutla's and P. Rogaway's proposals)

Stateless XCBC-XOR Scheme - Encryption of $x = x_1x_2x_3$



Example: $g(x) = x_1 \oplus x2 \oplus x3 \oplus z'_0$; $z'_0 = z_0$

Other examples of g(x) exist

Selection Criteria for S_i, op, g(x) ?

Satisfy Security Claims:

- Proof for integrity goal: EF-CPA

(*must be able to do the proofs for selected S_i, op, g(x)*):

• integrity: [GD 00]

Satisfy Operational Claims:

- Goals: low- to mid-end environments

Performance Example (by Jason S. Papadopoulos)

PC: 366 MHz Intel Celeron; OS: Red Hat Linux 5.2;
Compiler: egcs; optimization: -o3-mcpu = I686 - fomit - frame - pointer
Block Enc/Dec : openSSL DES

in-cache timing : 64B, 256B, 512B, 1KB, 2KB, 4KB, 8KB, 16KB, 64KB, 256 KB

- aligned data on 8 byte boundary

CBC-UMAC-MMX30	**42.86 - 46.48 clocks / byte; and for 8B - 77.23 clocks/byte**
XCBC-XOR	**43.38 - 44.62 clocks / byte; and for 8B - 49.57 clocks/byte**

- unaligned data (8 byte boundary +1)

CBC-UMAC-MMX30	**44.13 - 47.35 clocks / byte; and for 8B - 80.85 clocks/byte**
XCBC-XOR	**44.38 - 45.00 clocks / byte; and for 8B - 49.58 clocks/byte**

XECB - MAC

Motivation

- Stand-alone, fully parallel family of MACs, like the XOR-MAC
- **with better throughput**
- **reasonable security bounds for EF- CPA**

- XORC (and ctr-mode) needs a MAC with similar mode characteristics using the same cryptographic primitive

[XORC, and ctr-mode, does *not* allow non-cryptographic "redundancy" function g(x)]

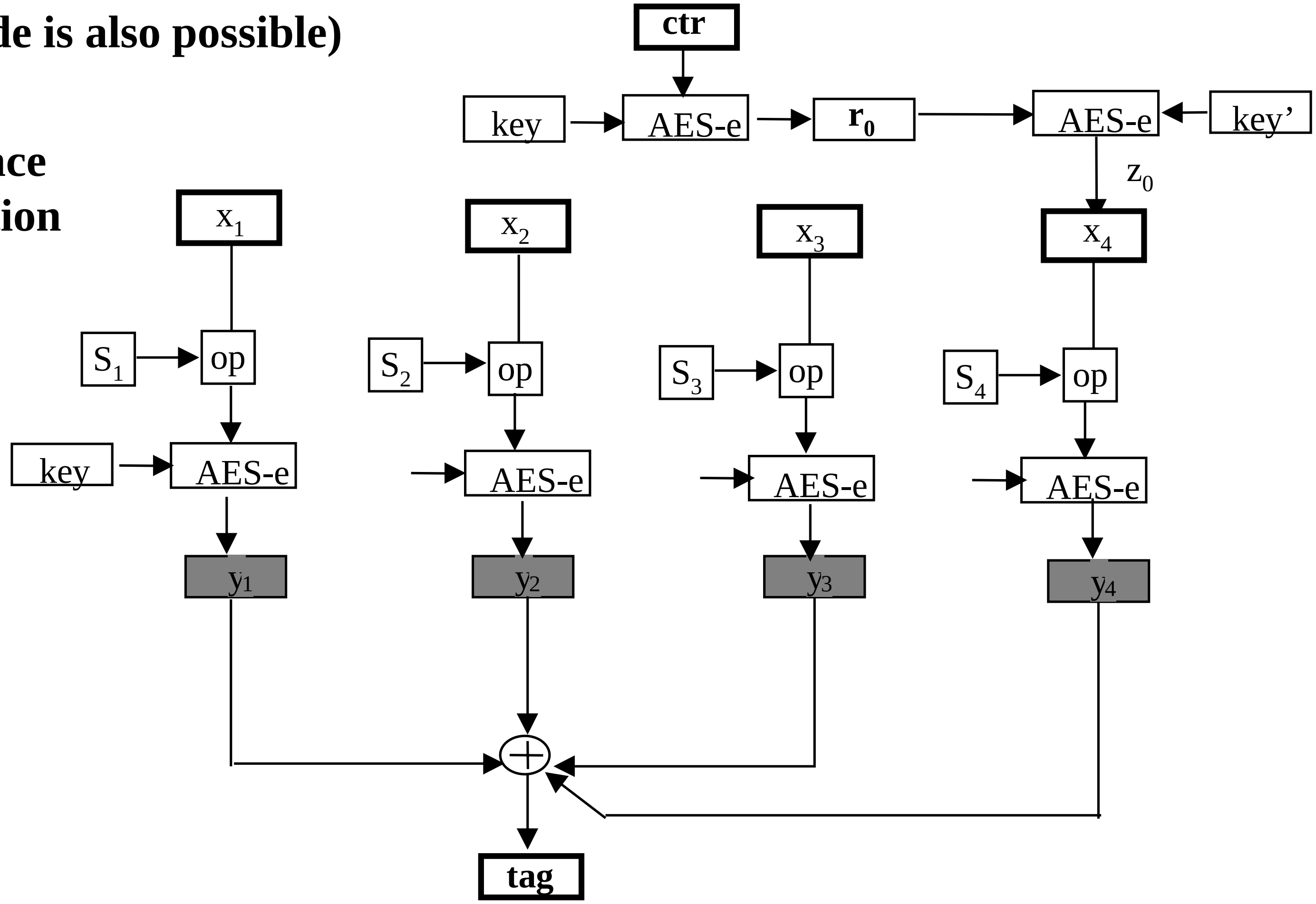
Preferred Operational Environment: High-End

- XORC (ctr-mode) + XECB (or any other similar MAC) requires two keys
=> two separate passes in *single processor*, *sequential* implementations
=> approx. twice the power consumption and half speed of XCBC-XOR

Stateful XECB - MAC: Example $x = x_1 x_2 x_3$

(single key mode is also possible)

S_i = sequence
op = operation



Examples of S_i and *op* combinations (+ is mod 2^l; $\oplus$ is bitwise exclusive-or)

op = + $S_i = S_{i-1} + r_0$, $S_0 = 0$ **(written as $S_i = i \times r_0$)**

op = $\oplus$ $S_i = S_{i-1} \times a$, $S_0 = r_0$ **(written as $S_i = a^i \times r_0$; *a* is a *lcs* constant)**

Other S_i and *op* definitions exist (e.g., P. Rogaway's PMAC)

Parallel Mode

Motivation

- Fully Parallel Mode like C.S. Jutla's IAPM using a different S_i
(S_i elements are *not* pairwise independent)

- Define family of parallel encryption modes to help provide integrity with non-cryptographic "redundancy" functions

- Security Claims (w/o proof) : IND-CPA confidentiality and EF-CPA integrity, reasonable bounds

Preferred Operational Environment: Mid- to High-End

- Single key for both Confidentiality and Integrity

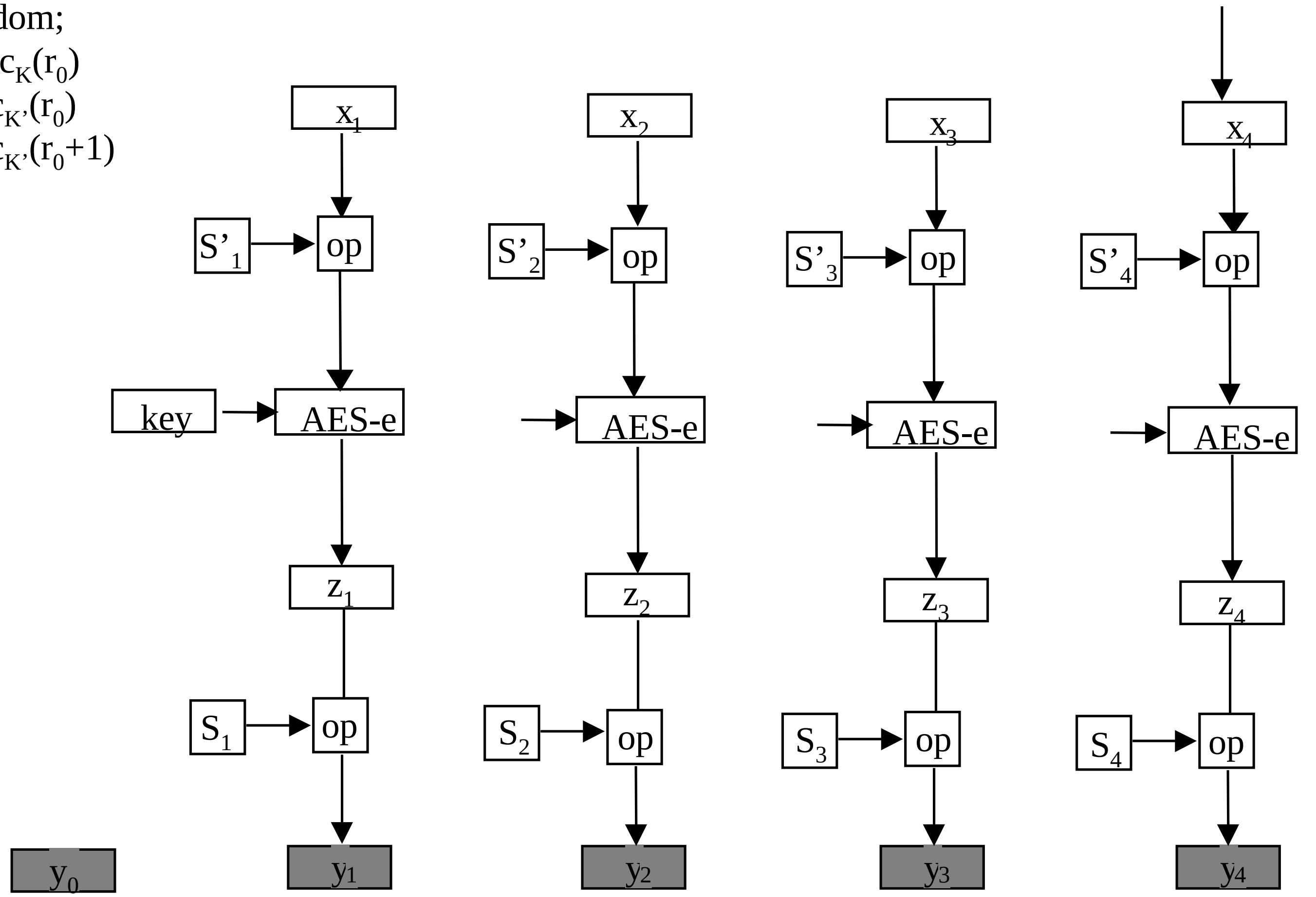
Stateless Parallel Mode - Encryption of $x = x_1x_2x_3$

(single key mode is also possible)

unpredictable function of message x

g(x)

r_0= random;
$y_0 = Enc_K(r_0)$
$z_0 = Enc_{K'}(r_0)$
$z_1 = Enc_{K'}(r_0+1)$



Example: $g(x) = x_1 \oplus x2 \oplus x3 \oplus z_0$;

$y_i = Enc_K(x_i + S'_i) + S_i$; $S'_i = i \times z_1$, $S_i = i \times r_0$; also use DESX if necessary

Other examples of S'_i, S_i, g(x) exist (e.g., C.S. Jutla's and P. Rogaway's proposals)

Proposal: Three* Distinct Modes of Operation

and Candidates (as of 10-18-2000)

• based on *preferred* environments of operation

1. ***Low- to Mid-End (very simple extensions of the venerable CBC)***

- **XCBC-XOR**
- **(possibly) interleaved mode**
- **IACBC**
- **XIGE-z_0 / XABC -z_0 (XCBC-like extensions of IGE / ABC)**

2. ***Mid- to High-End (single confidentiality and integrity key)***

- **IAPM**
- **PM-XOR**
- **OCB**

3. ***High-End (separate or independent key for confidentiality and integrity modes)***

- **ctr-mode for encryption**
- **XECB-MAC, PMAC for integrity**
- **(*) ctr-mode + XECB-MAC, ctr-mode + PMAC for both**

(*) the third mode of operation requires two separate AES modes

Intellectual Property Status

3 patent applications filed

Patent Application 1: on 1/31/2000

Patent Application 2: on 3/31/2000

Patent Application 3: on 8/24/2000