Reconciling Two Views of Cryptography

(The Computational Soundness of Formal Encryption)

Martin Abadi, Phillip Rogaway

Presented by:

Bushra, Justin, Nydia, Ryon

Outline

- Goal of the Paper
- Formal View of Encryption Schemes
- Computational View of Encryption Schemes
- Bridging the Gap

Formal View

$$\{M\}_K$$

Goals:

- How to convert between the formal view and the computational view.
- Proving equivalence implies indistinguishability.

Formal View

Expressions

EXP

M,N ::=	expressions
K	key (for *K* ∈ **Keys**)
i	bit (for *i* ∈ **Bool**)
(*M,N*)	pair
$\{M\}_K$	encryption (for *K* ∈ **Keys**)

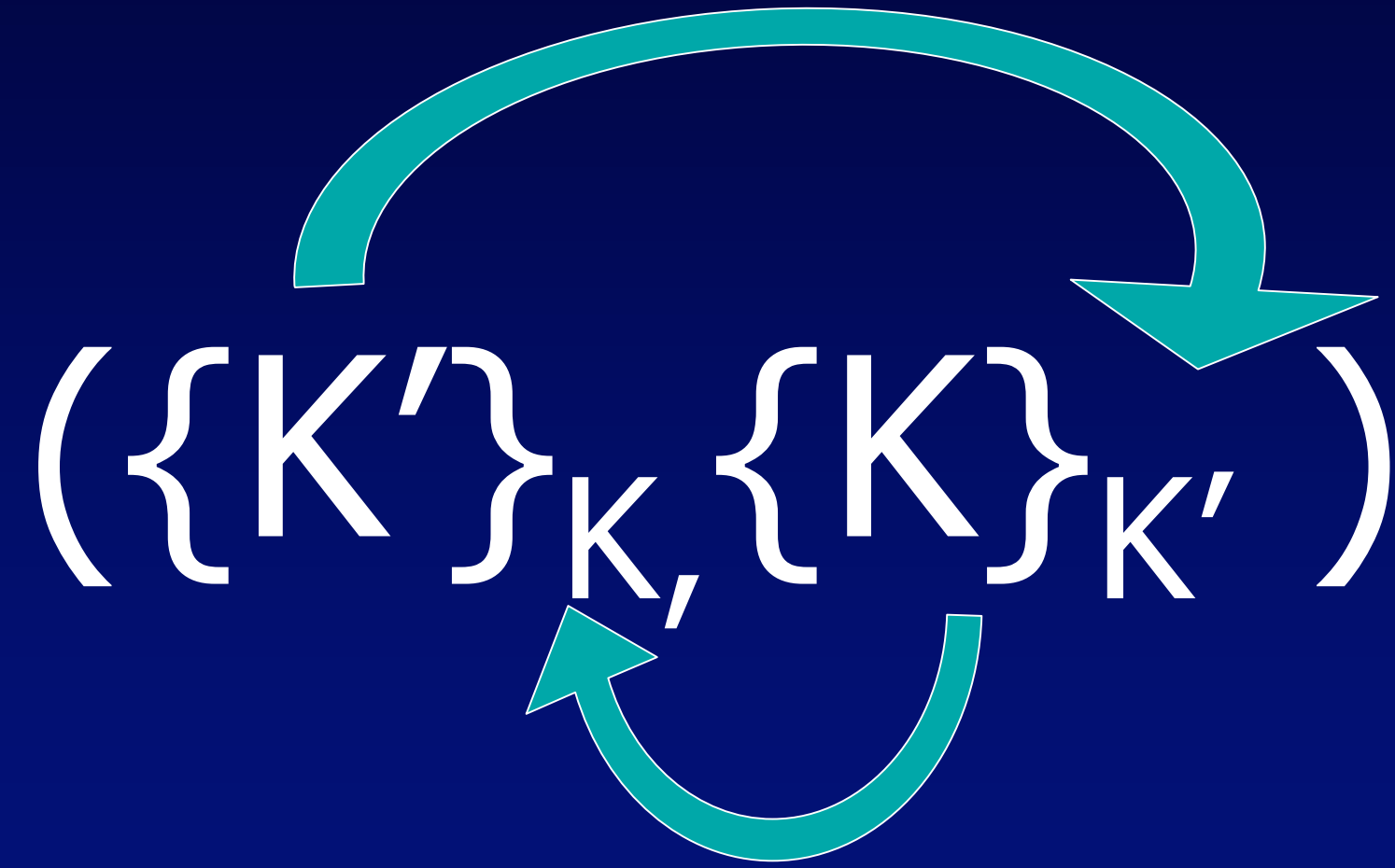
Formal View

EXP Example

$$(\{\{(0,K')\}_K\}_{K'},K)$$

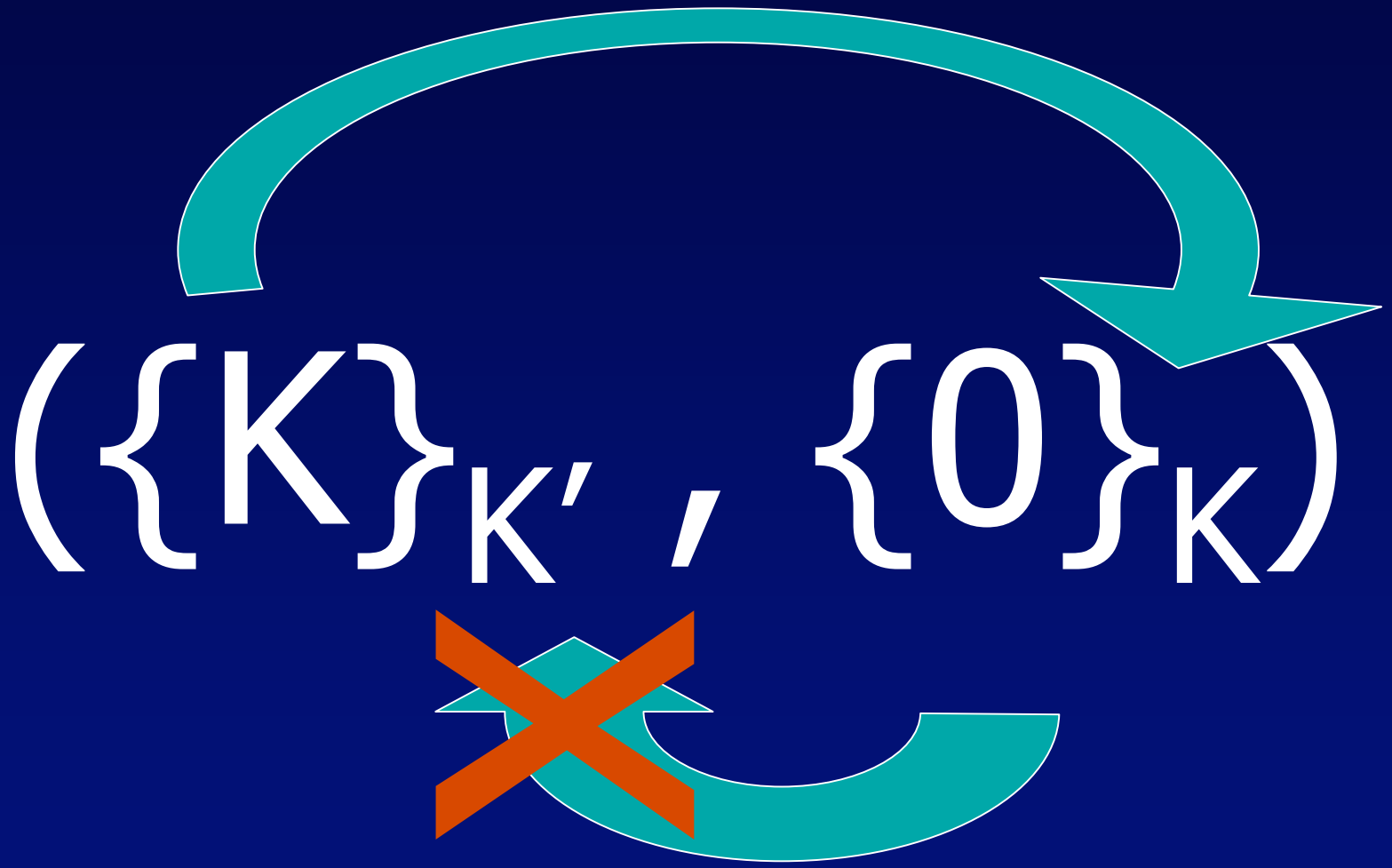
Formal View

Cyclic Expression



Formal View

Acyclic Expression



Formal View

Equivalence

Two expressions are said to be equivalent if they have the same patterns:

$M \equiv N$ if and only if *pattern* (M) = *pattern* (N)

Formal View

Pattern

Equivalent to **Exp**, but with the inclusion of the □ symbol.

□ - represents a ciphertext that an attacker cannot decrypt.

Formal View

$$(\{\{K_1\}_{K_2}\}_{K_3}, K_3) \equiv (\{\{0\}_{K_1}\}_{K_3}, K_3)$$

Formal View

Equivalent up to Renaming

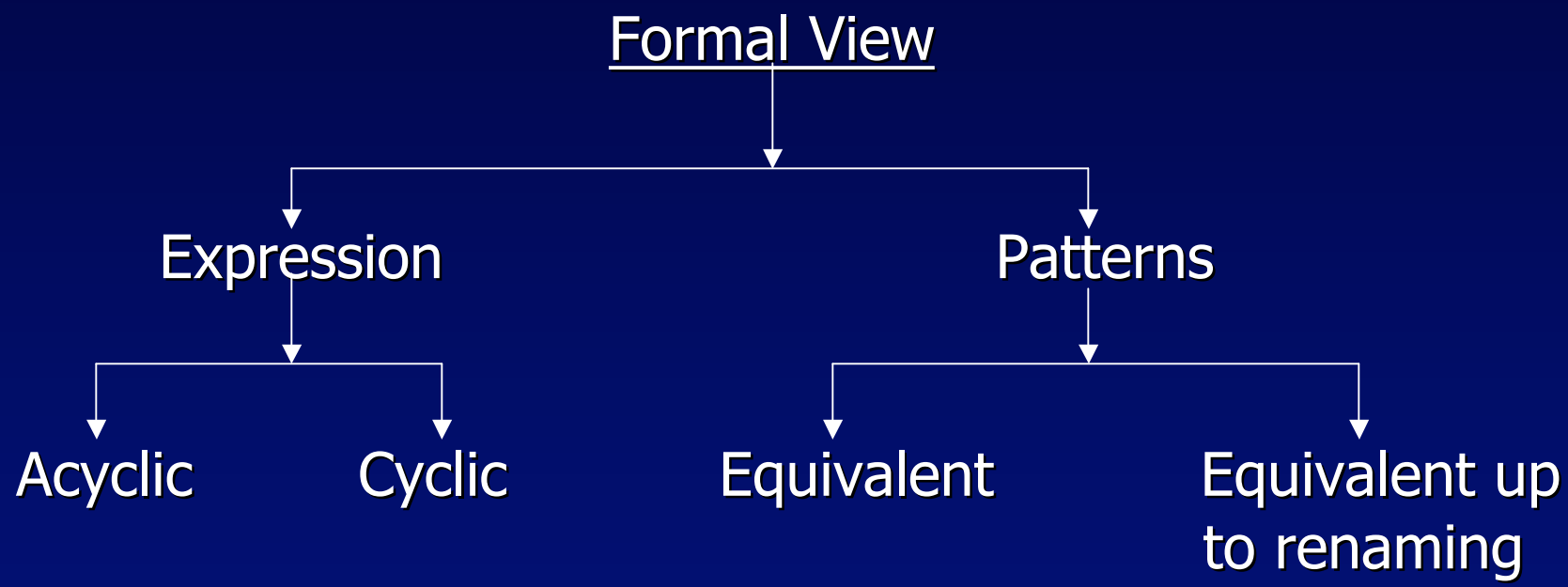
Two expressions are said to be equivalent up to renaming if there exists a bijection, σ, on **Keys**.

$$M \cong N \text{ if and only if } M \equiv N\sigma$$

Formal View

$$(\{O\}_K, K) \cong (\{O\}_{K'}, K')$$

Recap


Formal View
Expression
Patterns
Acyclic
Cyclic
Equivalent
Equivalent up to renaming

Computational View

Encryption Scheme: Π (K, ϵ , D)

K: Parameter x Coins $\rightarrow$ Key

ϵ : Key x String x Coins $\rightarrow$ Ciphertext

D: Key x String $\rightarrow$ Plaintext

where Parameter is represented by η

Computational View

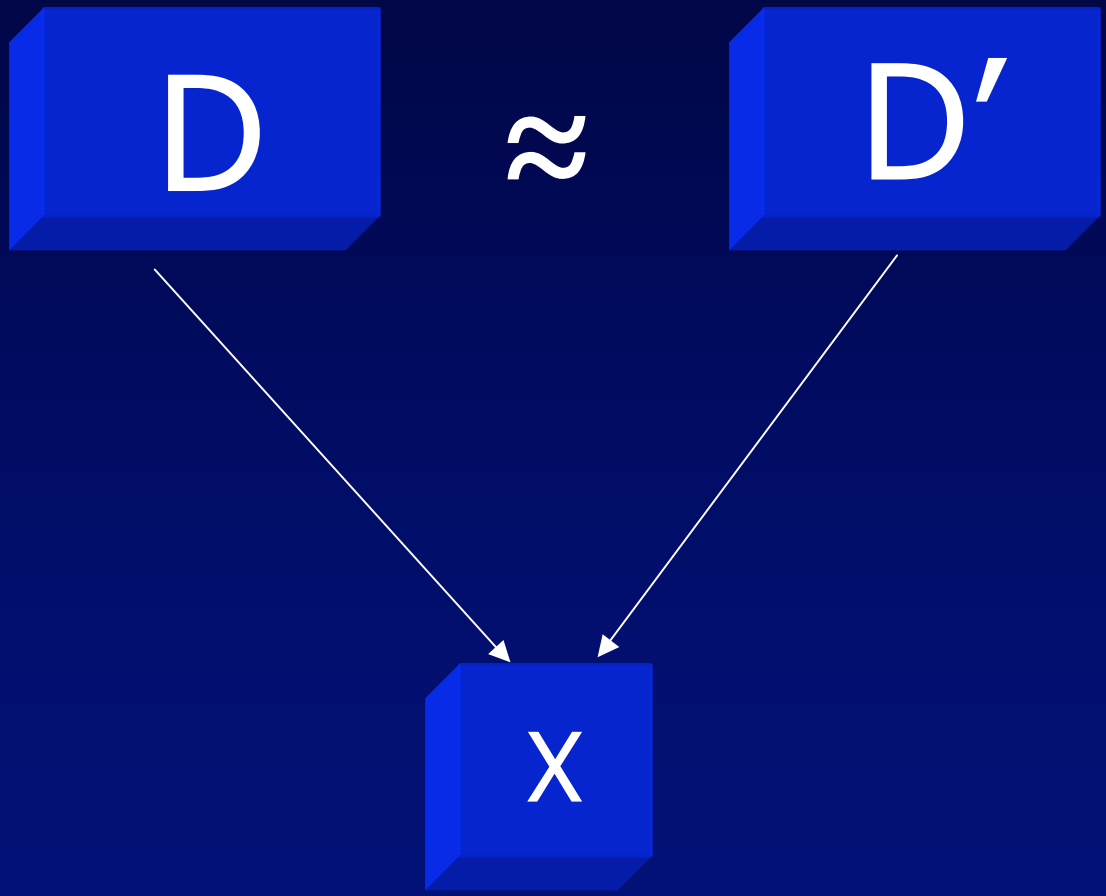
Ensemble

A collection of distributions on strings

$$D = \{D_\eta\}$$

Computational View

Indistinguishable



If an adversary cannot tell what set x is from

then D and D′ are indistinguishable.

Computational View

Attributes of Secure Encryption Schemes

- Repetition Concealing/ Revealing
- Which-key Concealing/ Revealing
- Message-length Concealing/ Revealing

Repetition Concealing/Revealing

- Given $c=E_k(x)$ and $d=E_k(x)$
- Can you tell whether the plaintext x is the same in both instances?

Which Key Concealing/Revealing

- Given $c=E_k(x)$ and $d=E_{k'}(x)$
- Can you tell whether k and k' are the same?

Message Length Concealing/Revealing

- Given $c=E_k(x)$ and $d=E_k(y)$
- Can you tell whether x and y are the same length?

Computational View

Security Types

- Represented as a 3-bit binary number, where concealing = 0 bit and revealing = 1 bit

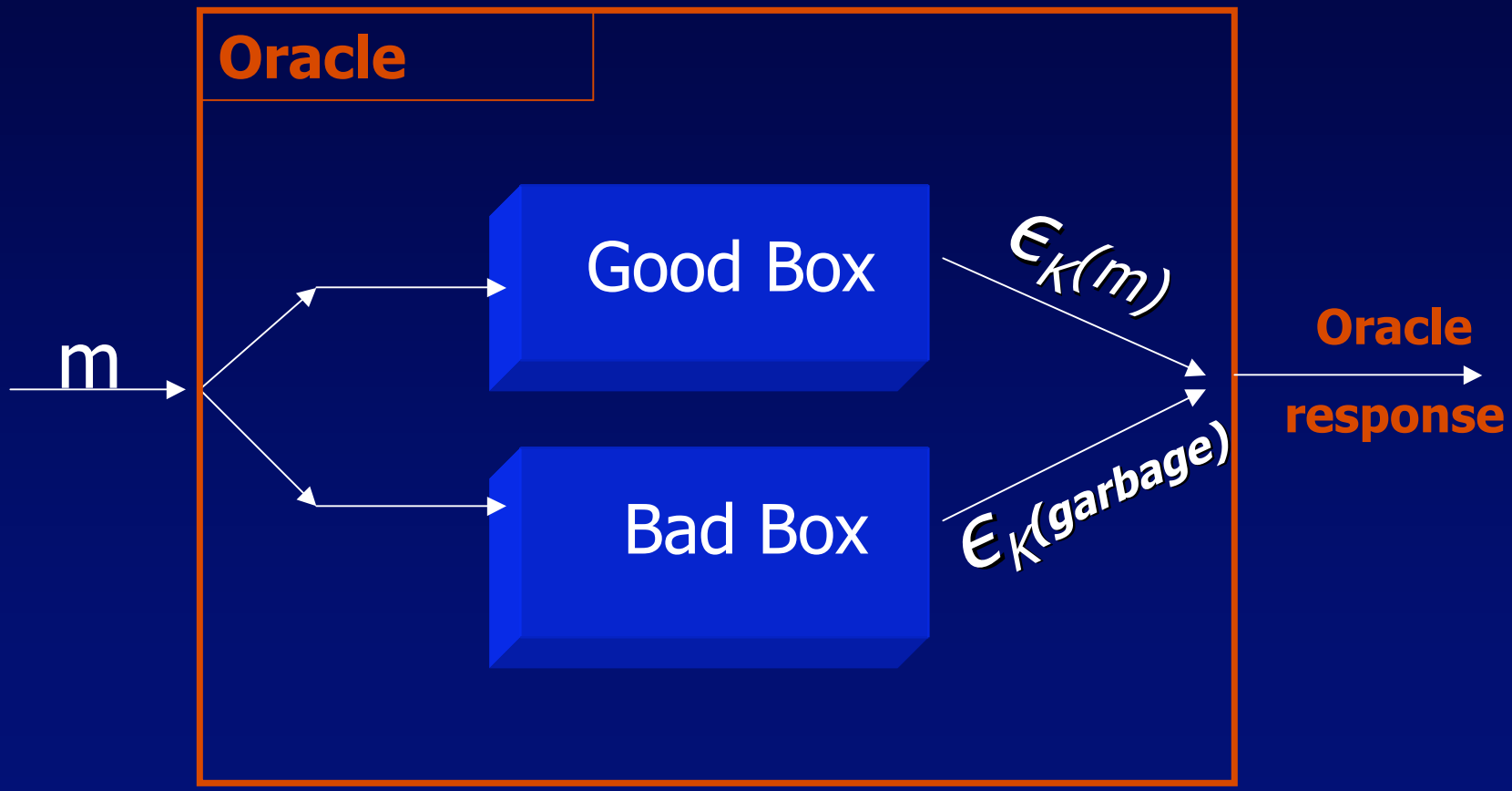
Example:

type-0 : 000 Repetition, Which-key and Message-length Concealing

type-3 : 011 Repetition concealing, Which-Key and Message-length Revealing

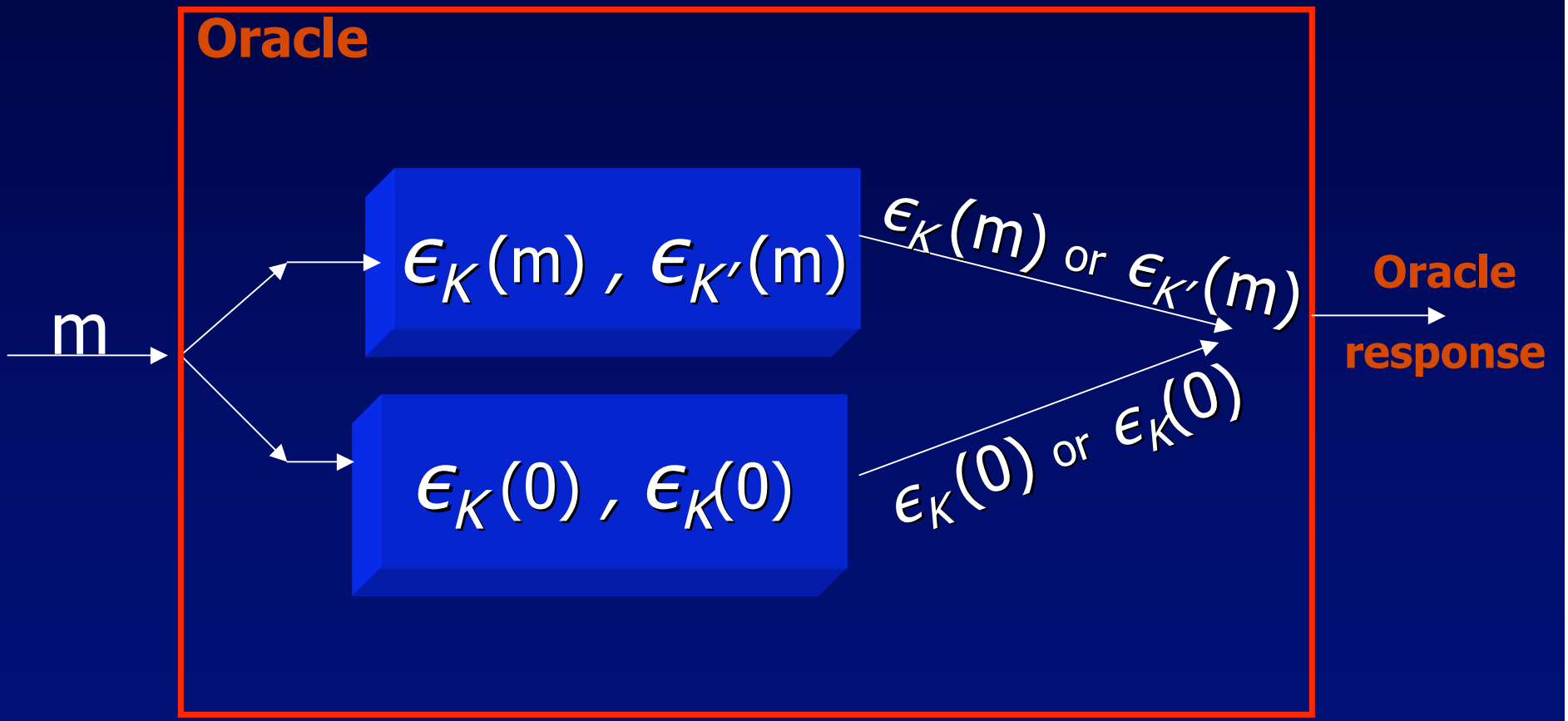
Computational View

Type-n Advantage



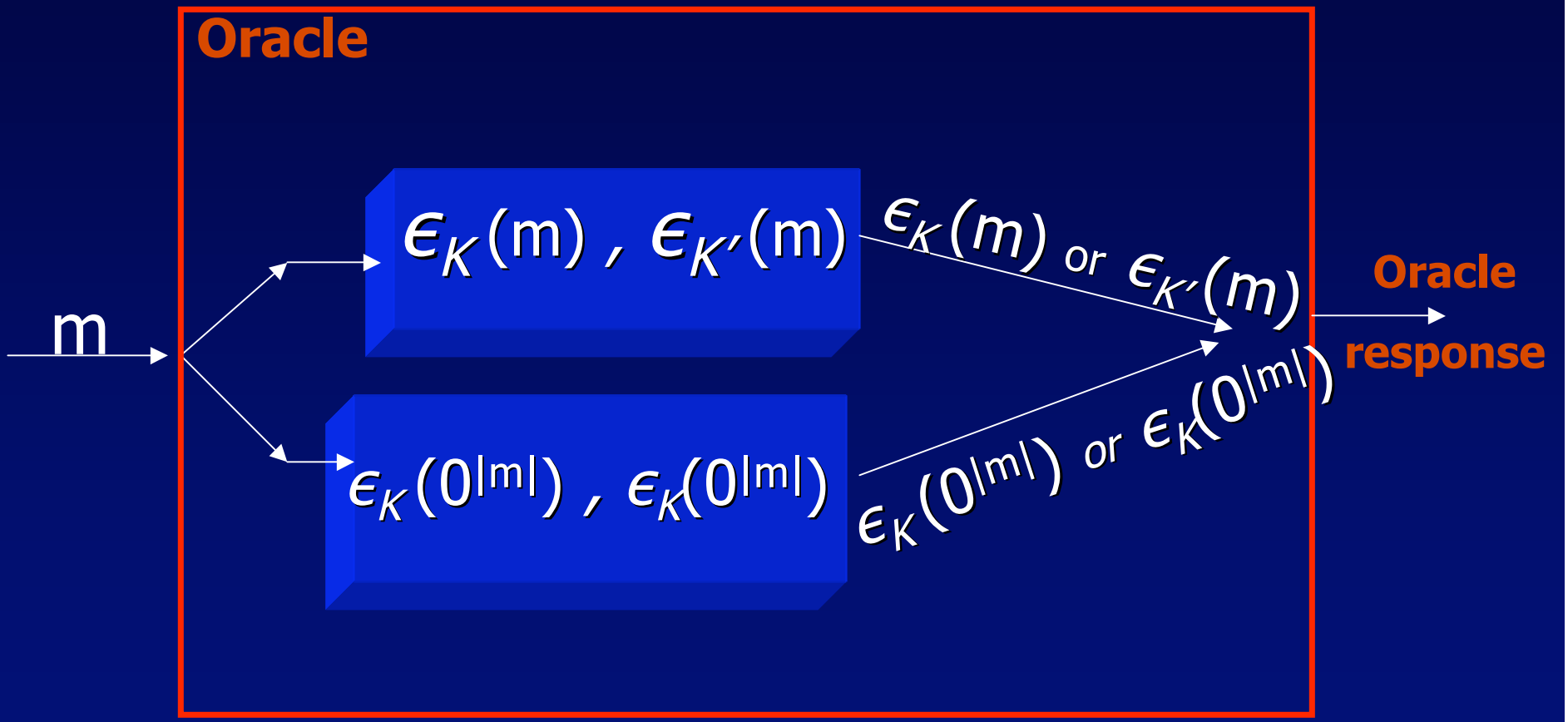
Computational View

type-0 Security Advantage



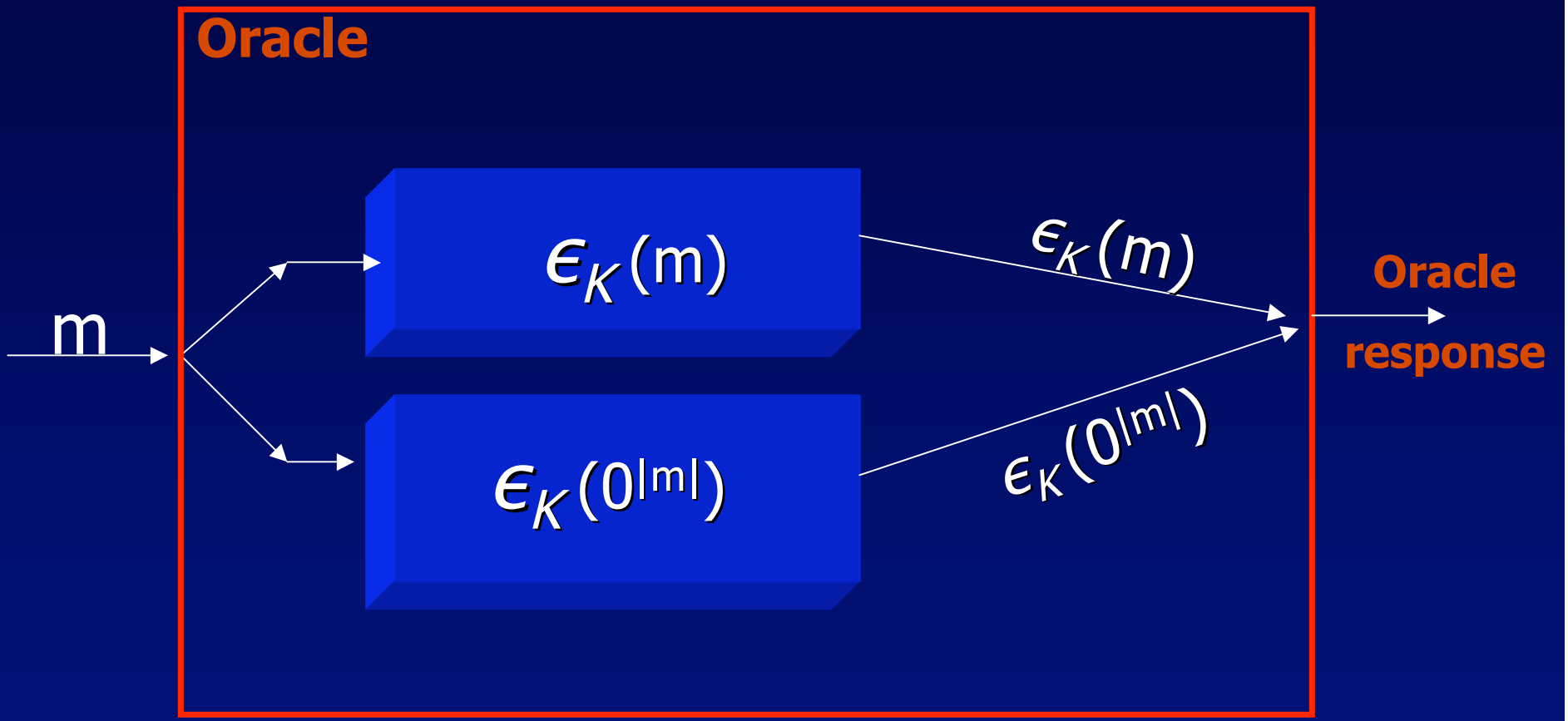
Computational View

type-1 Security Advantage



Computational View

type-3 Security Advantage



Computational View

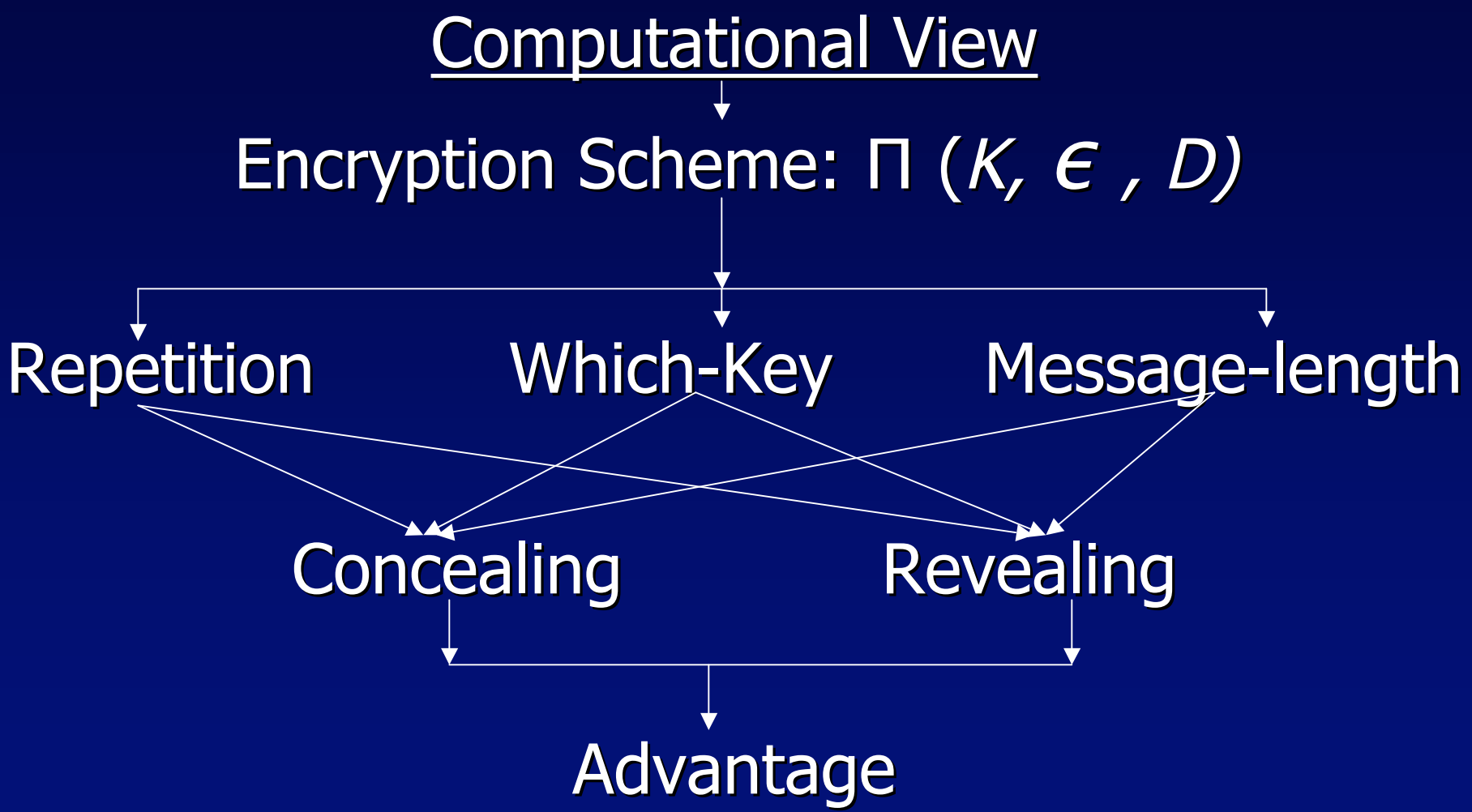
CTR mode is which–key concealing, message length revealing, repetition concealing

- Which-key, repetition
  - Cannot tell psuedorandom function from a random function
- Ciphertext length is same as plaintext

Hiding Message length for CTR?

- Make the plaintext some fixed length
- Then the plaintext is encrypted

Recap


Computational View
Encryption Scheme: Π (K, ϵ , D)
Repetition
Which-Key
Message-length
Concealing
Revealing
Advantage

Bridging the Gap

Relating the two views of Cryptography

Step 1. Associate an ensemble to an expression *M*, given an encryption scheme Π.

Step 2. Proving

equivalent expression implies indistinguishable ensembles

Expression -> Ensemble

Given:

formal expression $M \in \mathbf{EXP}$

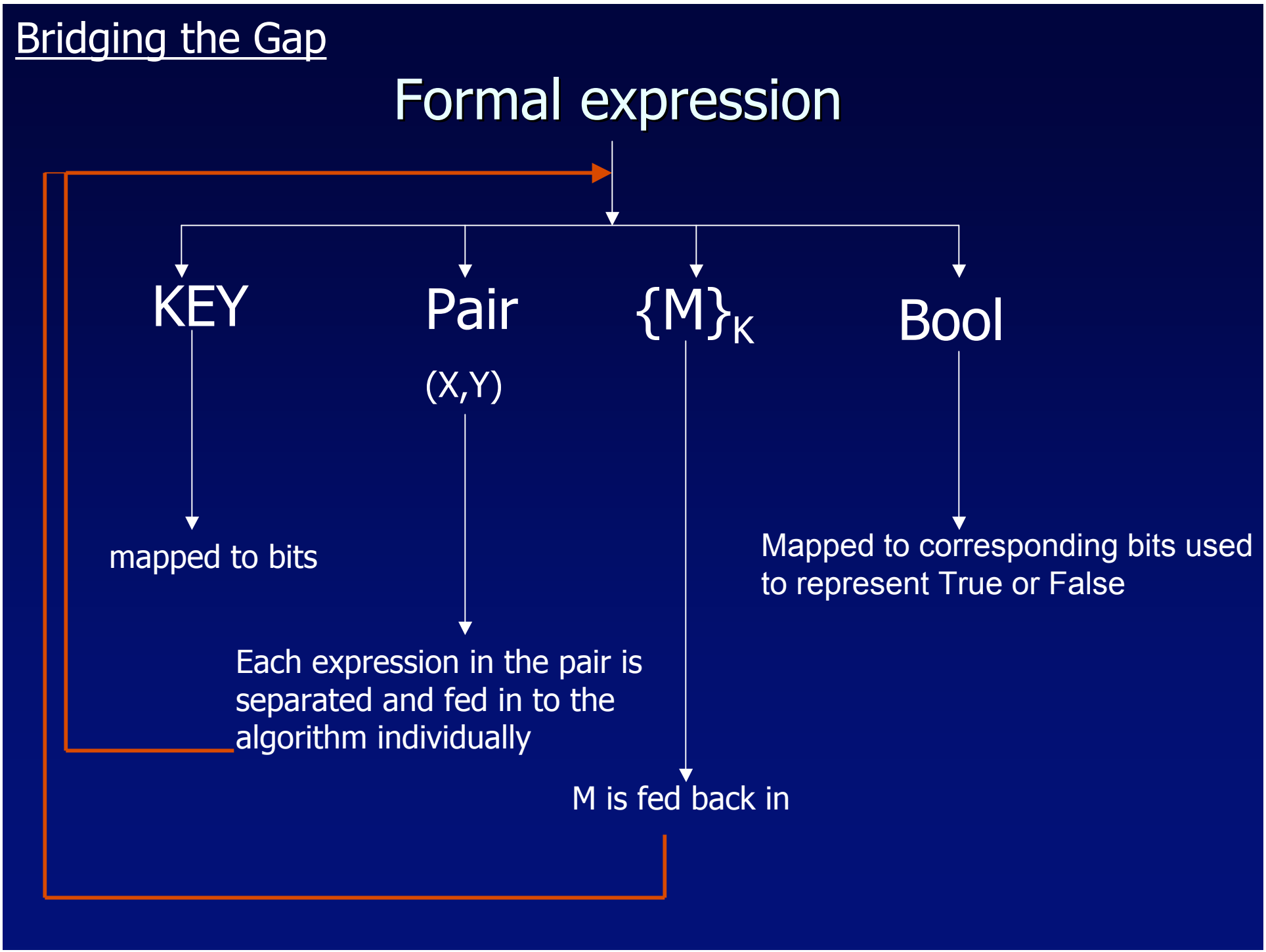
encryption scheme Π (K, E, D)

Then:

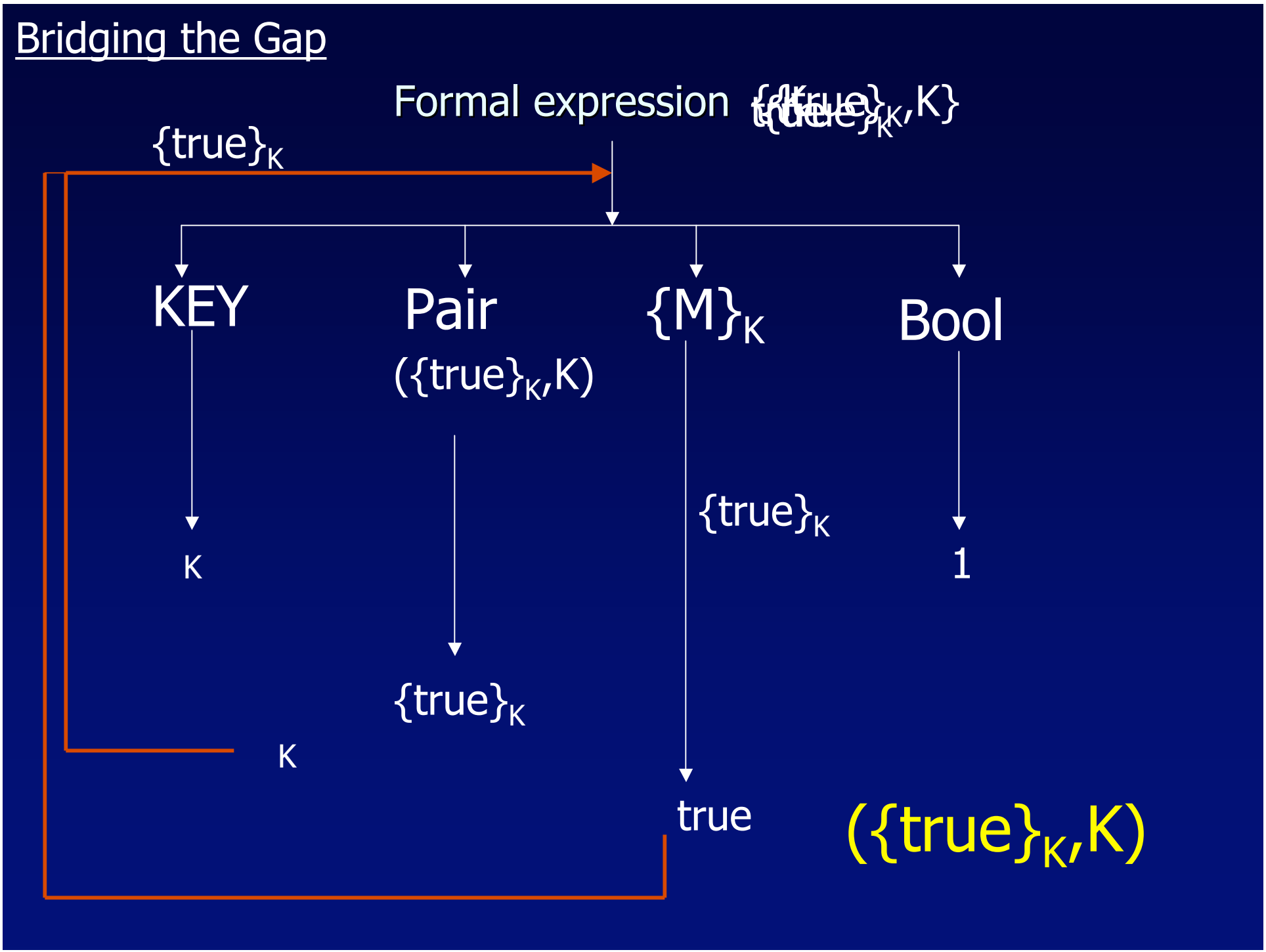
$[\![M]\!]_{\Pi[\eta]}$ • Distribution of strings

$[\![M]\!]_{\Pi}$ • Ensemble

Bridging the Gap



Bridging the Gap



The Theorem

"Let *M and N be acyclic expressions and let Π be a type-0 secure encryption scheme. Suppose that* $M \cong N$. *Then*

$$[\![M]\!]_{\Pi} \approx [\![N]\!]_{\Pi}$$ "

Proof to come….stay tuned…..