Indifferentiable Authenticated Encryption

Manuel Barbosa
(Porto)

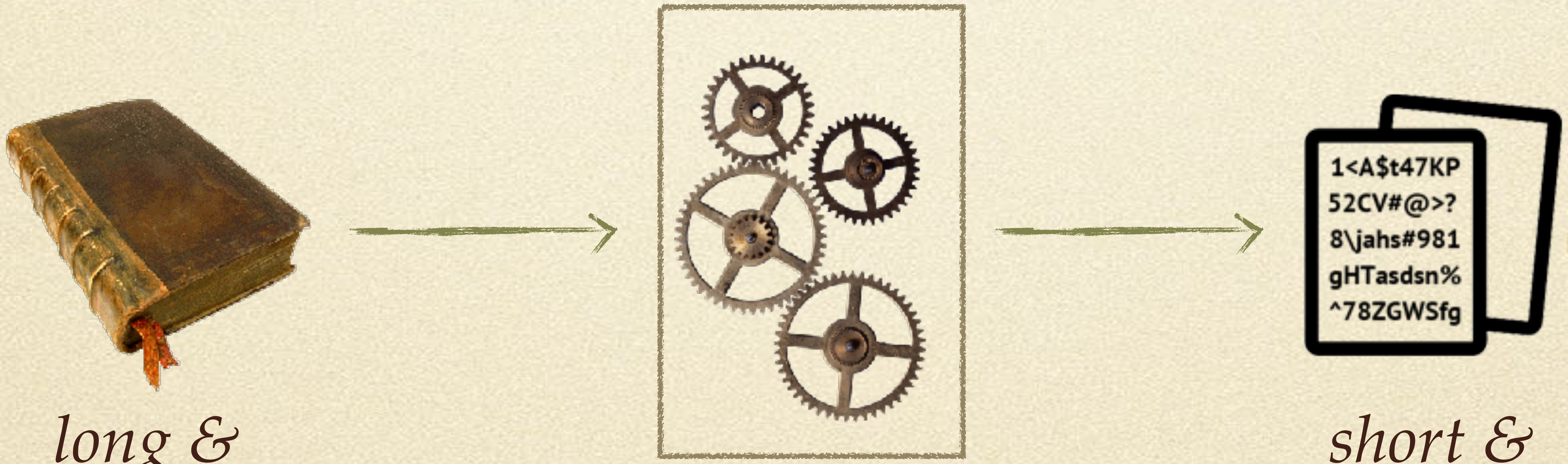
Pooya Farshim
(CNRS & ENS)

Indifferentiable Authenticated Encryption

Manuel Barbosa

Pooya Farshim
(CNRS & ENS)

Hash Functions

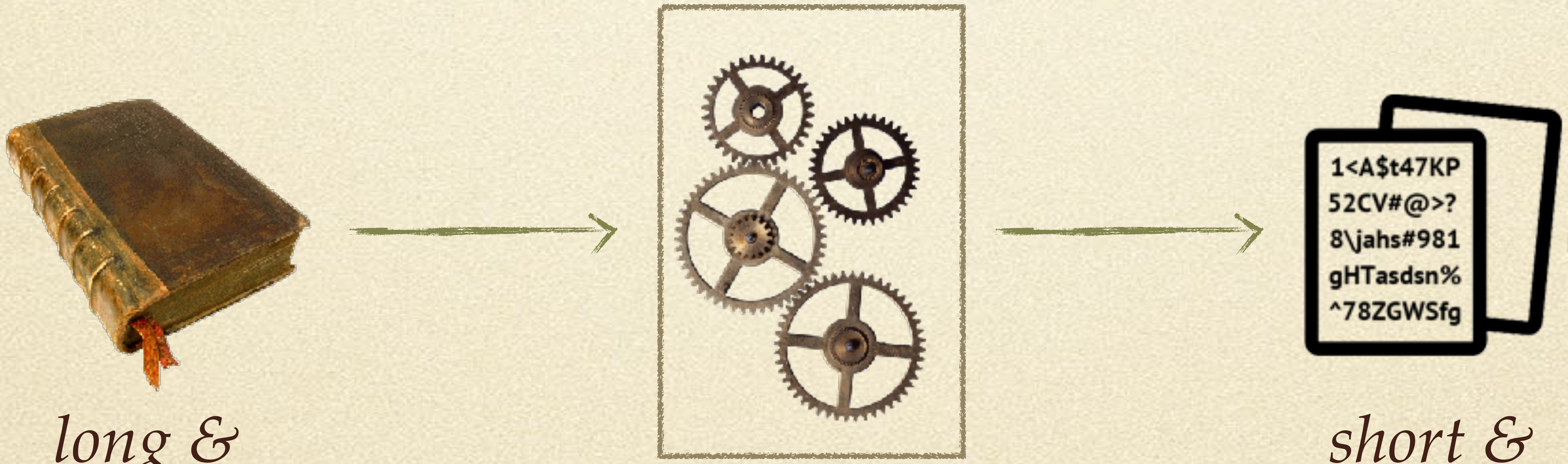


long & arbitrary

SHA

short & random-looking

Hash Functions



long & arbitrary

SHA

short & random-looking

Provably security not always possible.

Random Oracles

long & arbitrary

SHA

short & random-looking

Random Oracles

long &
arbitrary

Random Function

short &
random-looking

Random Oracles

long & arbitrary

Random Oracle

short & random-looking

Random Oracles are Practical

Ideal Hash

Provable Security for
Many Simple & Efficient Protocols

- Public-Key Enc. (OAEP, ECIES)
- Signatures (PSS, FDH)
- TLS 1.3
- Symmetric schemes
- ….

This Talk

This Talk

Encryption

This Talk

Ideal Hash

$\downarrow$

Encryption

This Talk

Ideal Hash

Inherit
all strengths

Encryption

This Talk

Ideal Hash

Inherit
all strengths

Ideal Encryption

This Talk

Ideal Hash

Random
Function

Inherit
all strengths

Ideal Encryption

This Talk

Ideal Hash ⟷ *Random Function*

Inherit all strengths

↓

Ideal Encryption ⟷ *What Object?*

Authenticated Encryption

Authenticated Encryption

1. $K \twoheadleftarrow \text{Gen}(1^\lambda)$
2. $C \leftarrow \text{Enc}(K,N,A,M,\tau)$ $\quad |C| = |M| + \tau$
3. $M/\perp \leftarrow \text{Dec}(K,N,A,C,\tau)$

Authenticated Encryption

1. $K \twoheadleftarrow \mathrm{Gen}(1^\lambda)$
2. $C \leftarrow \mathrm{Enc}(K,N,A,M,\tau) \quad |C| = |M| + \tau$
3. $M/\perp \leftarrow \mathrm{Dec}(K,N,A,C,\tau)$

Security says: under an unknown random key K

- *Nothing about messages leaks*
- *Cannot forge new valid ciphertexts*

Simplifying

1. $K \twoheadleftarrow \mathrm{Gen}(1^\lambda)$
2. $C \leftarrow \mathrm{Enc}(K,M) \quad |C| = |M| + \tau$
3. $M/\perp \leftarrow \mathrm{Dec}(K,C)$

Simplifying

1. $K \twoheadleftarrow \mathrm{Gen}(1^\lambda)$
2. $C \leftarrow \mathrm{Enc}(K,M) \quad |C| = |M| + \tau$
3. $M/\perp \leftarrow \mathrm{Dec}(K,C)$

A Keyed Injection

Ideal Encryption

Ideal Encryption

Hash

Ideal Encryption

Hash ⟷ *Function*

Ideal Encryption

Ideal Hash $\longleftrightarrow$ Function

Ideal Encryption

Ideal Hash ⟷ *Random Function*

Ideal Encryption

Ideal Hash Cipher ⟷ *Random Function*

Ideal Encryption

Ideal Hash	$\longleftrightarrow$	*Random Function*
Cipher	$\longleftrightarrow$	*Keyed Permutation*

Ideal Encryption

Ideal Hash	$\longleftrightarrow$	Random Function
Ideal Cipher	$\longleftrightarrow$	Keyed Permutation

Ideal Encryption

Ideal Hash	⟷	Random Function
Ideal Cipher	⟷	Random Keyed Permutation

Ideal Encryption

Ideal Hash ⟷ Random Function
Ideal Cipher ⟷ Random Keyed Permutation
Encryption

Ideal Encryption

Ideal Hash	⟷	Random Function
Ideal Cipher	⟷	Random Keyed Permutation
Encryption	⟷	Keyed Injection

Ideal Encryption

Ideal Hash	⟷	Random Function
Ideal Cipher	⟷	Random Keyed Permutation
Ideal Encryption	⟷	Keyed Injection

Ideal Encryption

Ideal Hash	$\longleftrightarrow$	Random Function
Ideal Cipher	$\longleftrightarrow$	Random Keyed Permutation
Ideal Encryption	$\longleftrightarrow$	Random Keyed Injection

Ideal Encryption

Ideal Hash	⟷	Random Function
Ideal Cipher	⟷	Random Keyed Permutation
Ideal Encryption	⟷	Random Keyed Injection

New
Ideal Model

Encryption

Ideal Hash ⟷ Random Function

Inherit all strengths

Ideal Encryption ⟷ What Object?

Encryption

Ideal Hash ⟷ Random Function

Inherit all strengths ↓

Ideal Encryption ⟷ Random Keyed Injection

Encryption

Ideal Hash ⟷ *Random Function*

Inherit all strengths

Ideal Encryption ⟷ *Random Keyed Injection*

Encryption

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\text{Ideal Hash} \arrow[r, leftrightarrow] \arrow[d, "\text{Inherit all strengths}"'] & \text{Random Function} \arrow[d, "\text{Indifferentiability}"] \\
\text{Ideal Encryption} \arrow[r, leftrightarrow] & \text{Random Keyed Injection}
\end{tikzcd}$$

Indifferentiability

C^{RO} is "as good as" iEnc:

Indifferentiability

C^{RO} is "as good as" iEnc:

$$C^{RO} \approx iEnc$$

Indifferentiability

C^{RO} *is "as good as" iEnc:*

$$C^{RO}, RO \quad \approx \quad iEnc$$

Indifferentiability

C^{RO} *is "as good as" iEnc:*

$$C^{RO}, RO \quad \approx \quad iEnc\,, RO$$

Indifferentiability

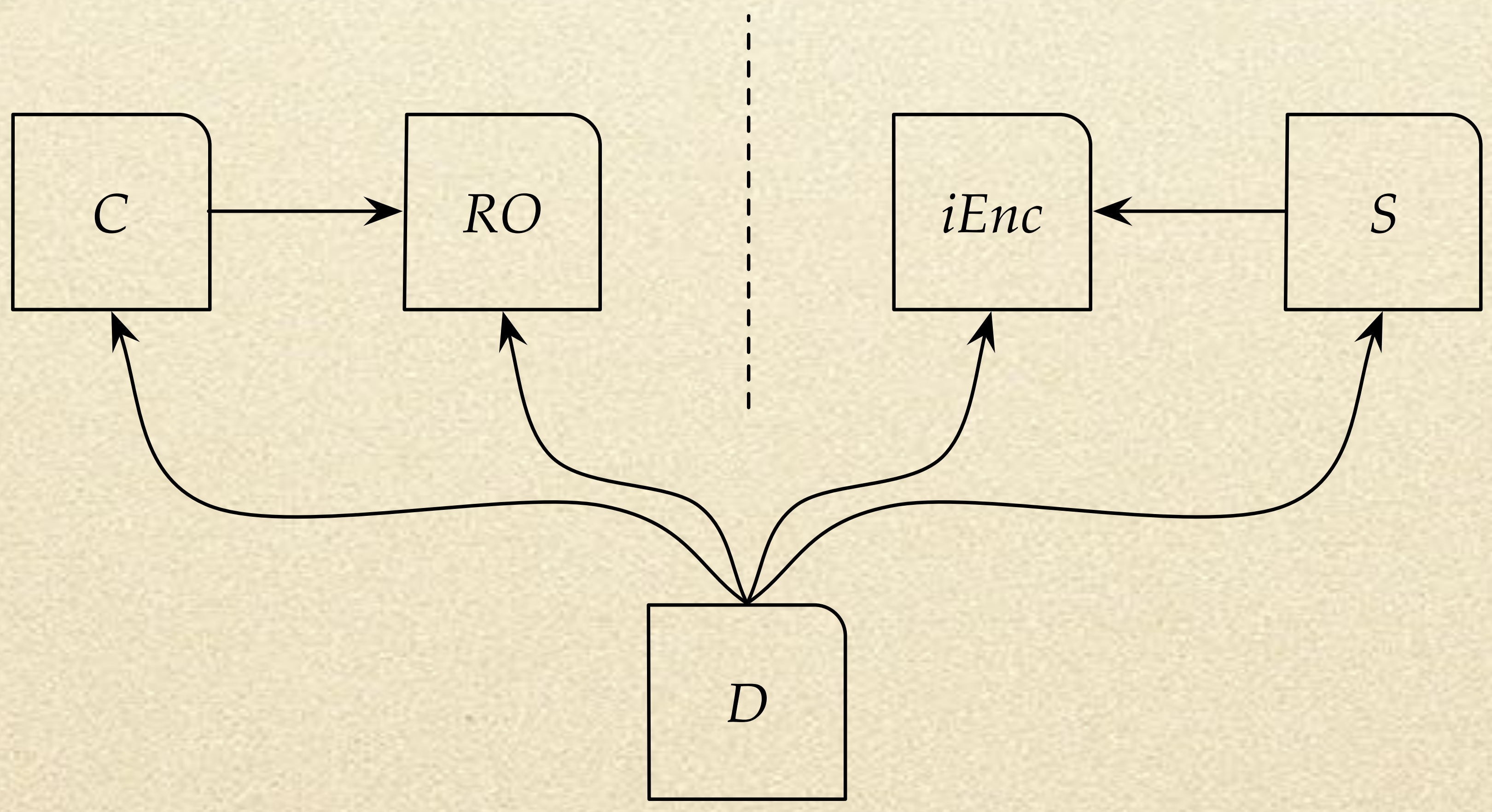
C^{RO} *is "as good as" iEnc:*

$$C^{RO}, RO \quad \approx \quad iEnc, S^{iEnc}$$

Indifferentiability

C^{RO} is "as good as" iEnc:

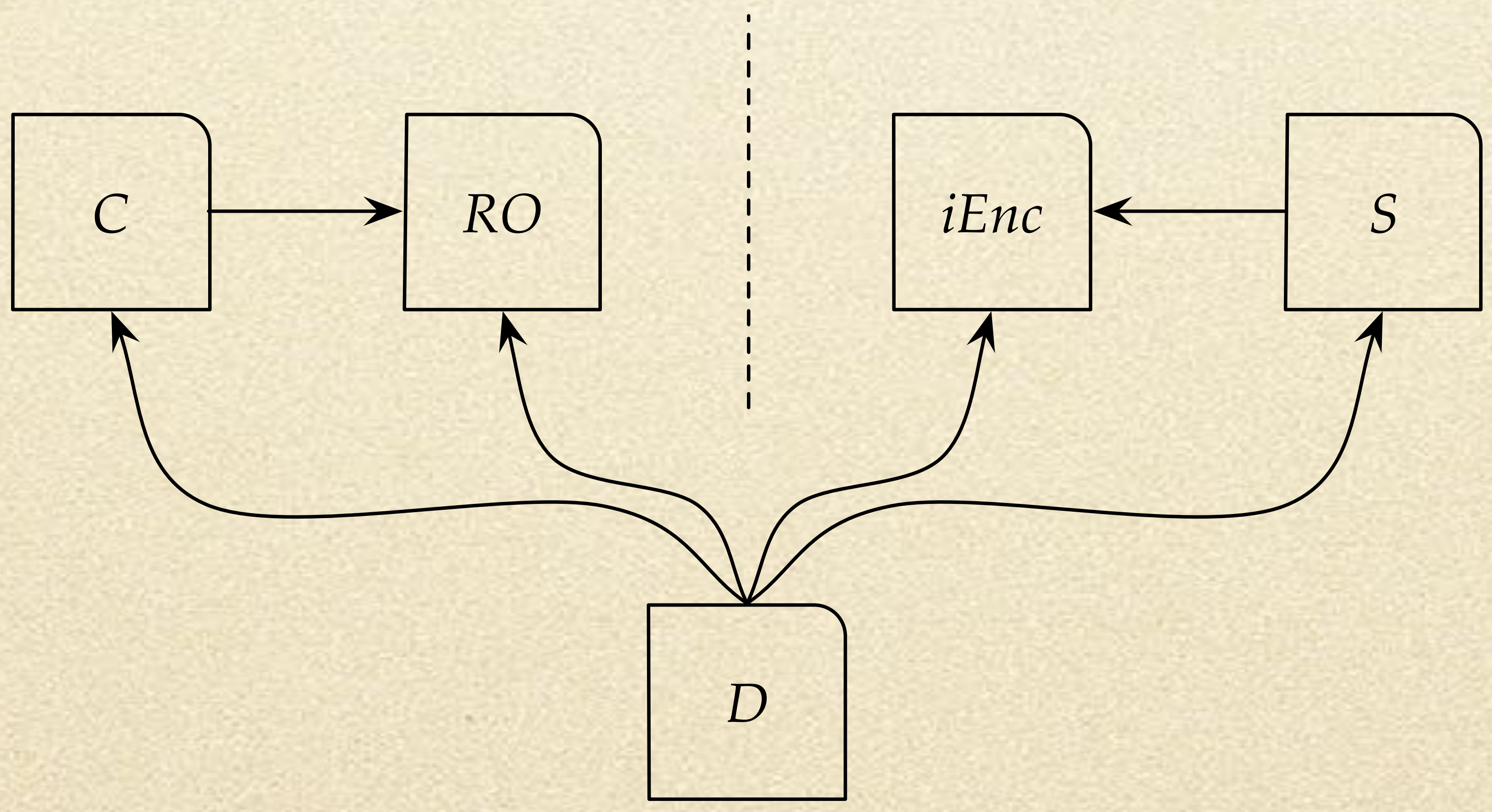
$$C^{RO}, RO \quad \approx \quad iEnc, S^{iEnc}$$



Indifferentiability

C^{RO} is "as good as" iEnc:

$$C^{RO}, RO \quad \approx \quad iEnc, S^{iEnc}$$

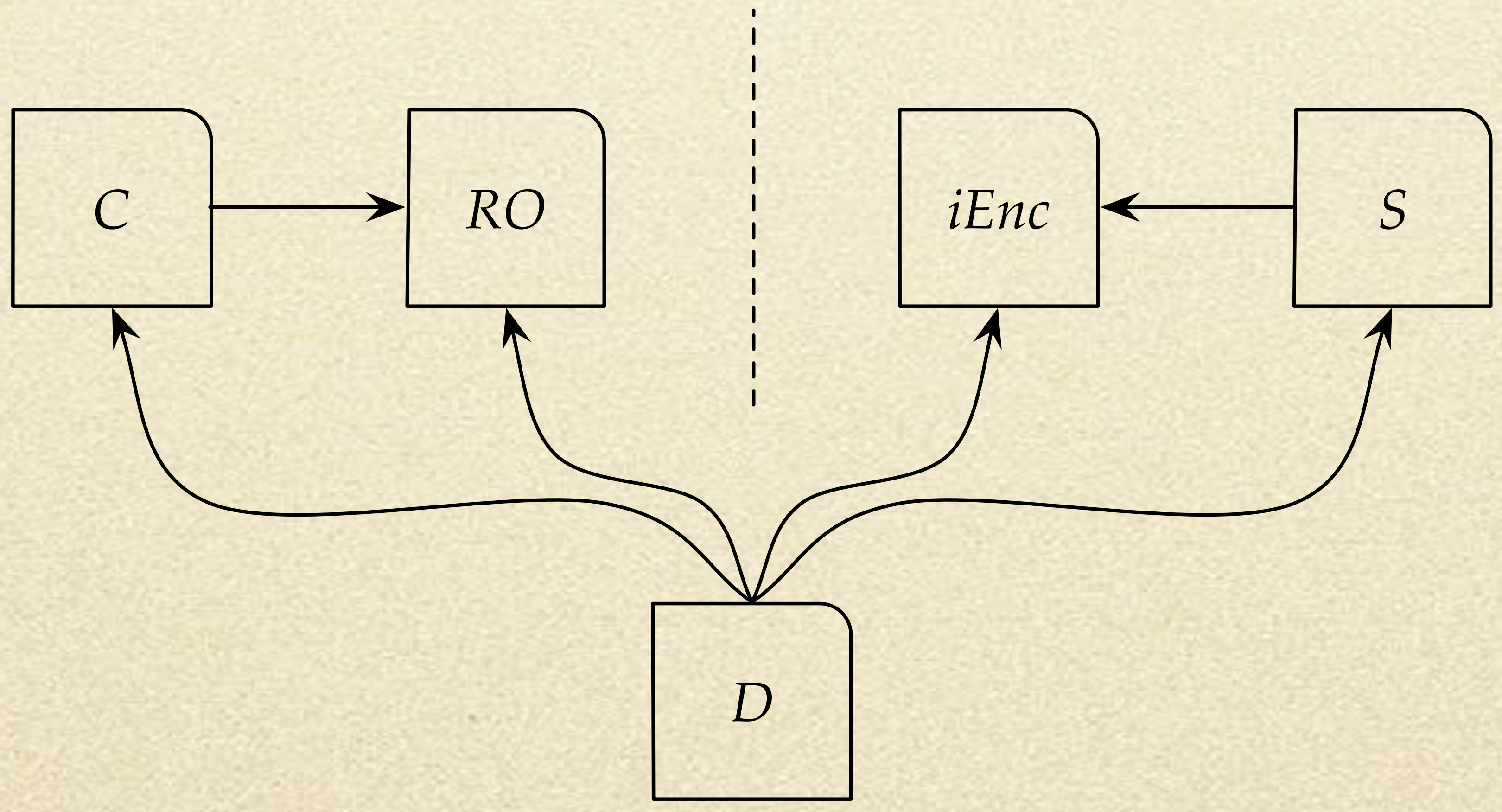


Unified Attack Surface

Indifferentiability

C^{RO} is "as good as" iEnc:

$$C^{RO}, RO \quad \approx \quad iEnc, S^{iEnc}$$



Keys can be under adversarial control

Unified Attack Surface

Why Indifferentiability?

Theorem [MRH04]: *If C^{RO} is indifferentiable from iEnc, then it is secure in many adversarial environments in the RO model.*

Why Indifferentiability?

Theorem [MRH04]: *If C^{RO} is indifferentiable from iEnc, then it is secure in many adversarial environments in the RO model.*

AE, MRAE, & RAE

Why Indifferentiability?

Theorem [MRH04]: *If C^{RO} is indifferentiable from iEnc, then it is secure in many adversarial environments in the RO model.*

AE, MRAE, & RAE

KDM Security

Leakage Resilience

RKA Security

Committing Encryption

Deduplication

Why Indifferentiability?

Theorem [MRH04]: *If C^{RO} is indifferentiable from iEnc, then it is secure in many adversarial environments in the RO model.*

AE, MRAE, & RAE

KDM Security

Leakage Resilience

RKA Security

Committing Encryption

Deduplication

Combined Models

Unforeseen Models

Why Indifferentiability?

Theorem [MRH04]: *If C^{RO} is indifferentiable from iEnc, then it is secure in many adversarial environments in the RO model.*

AE, MRAE, & RAE

KDM Security

Leakage Resilience

RKA Security

Committing Encryption

Deduplication

Combined Models

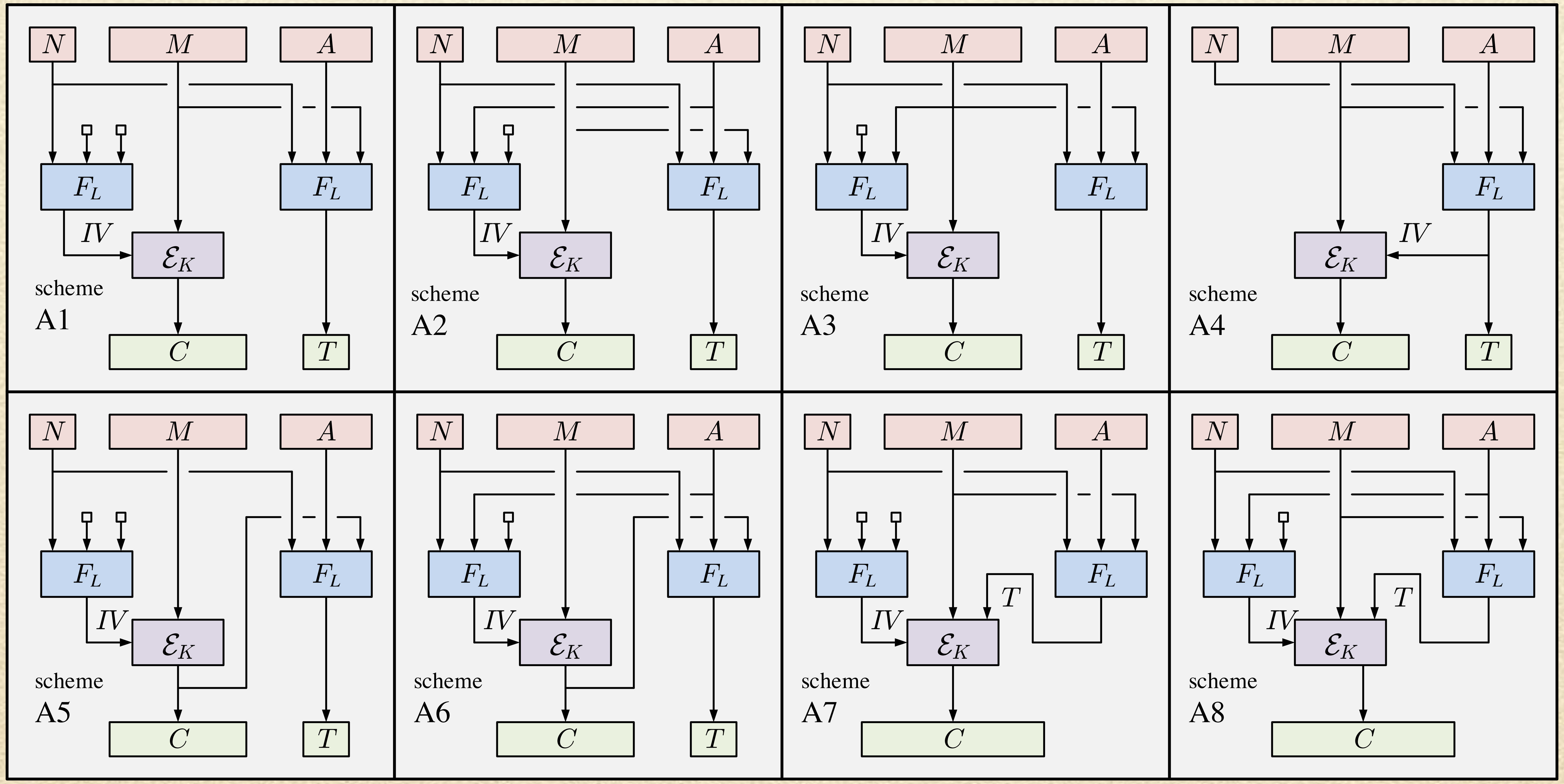
Unforeseen Models

Single stage

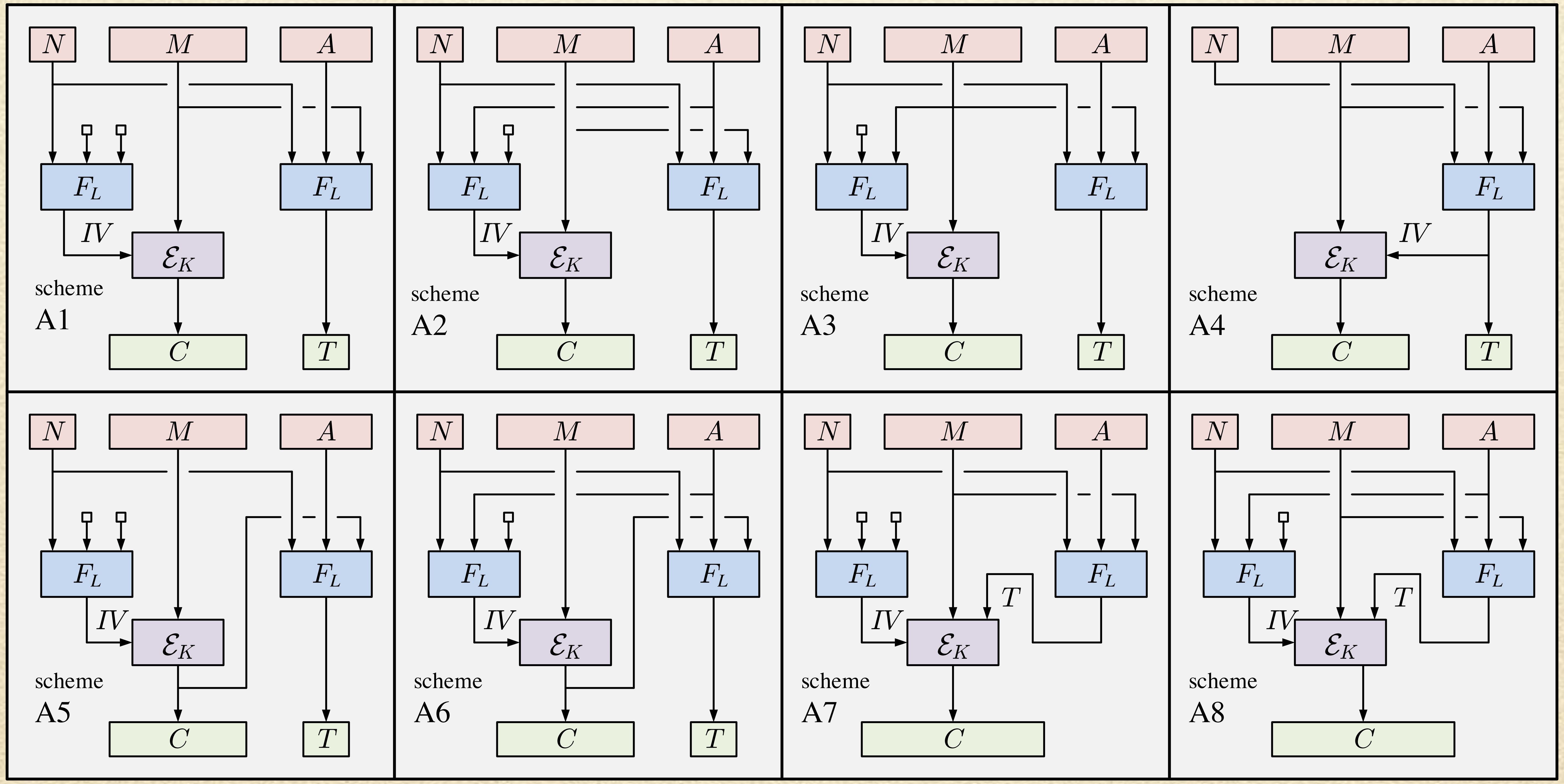
So…

Are there any indifferentiable encryption schemes out there?

Generic Composition [NRS14]

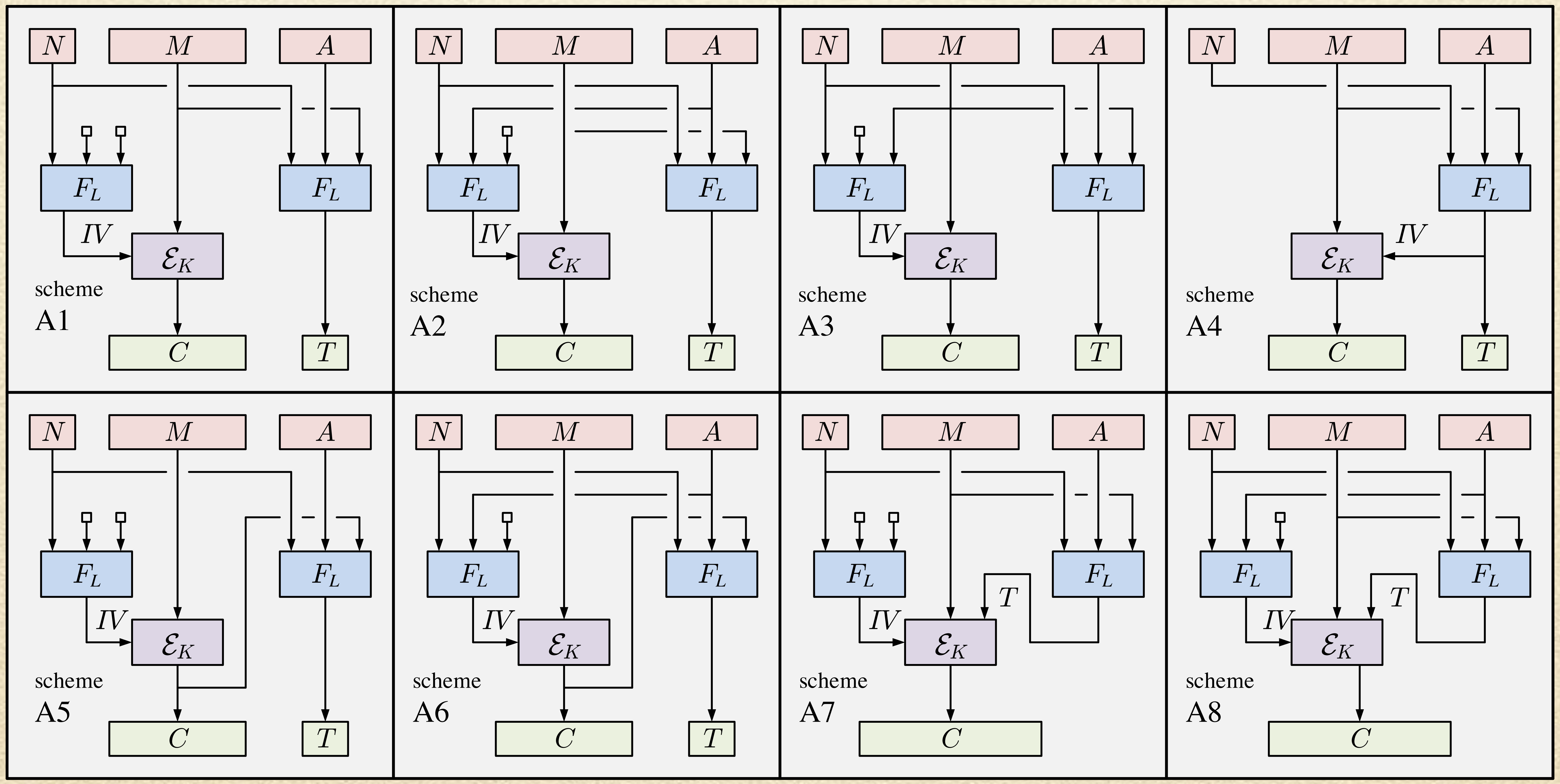


Generic Composition [NRS14]



Enc-then-Mac

Generic Composition [NRS14]

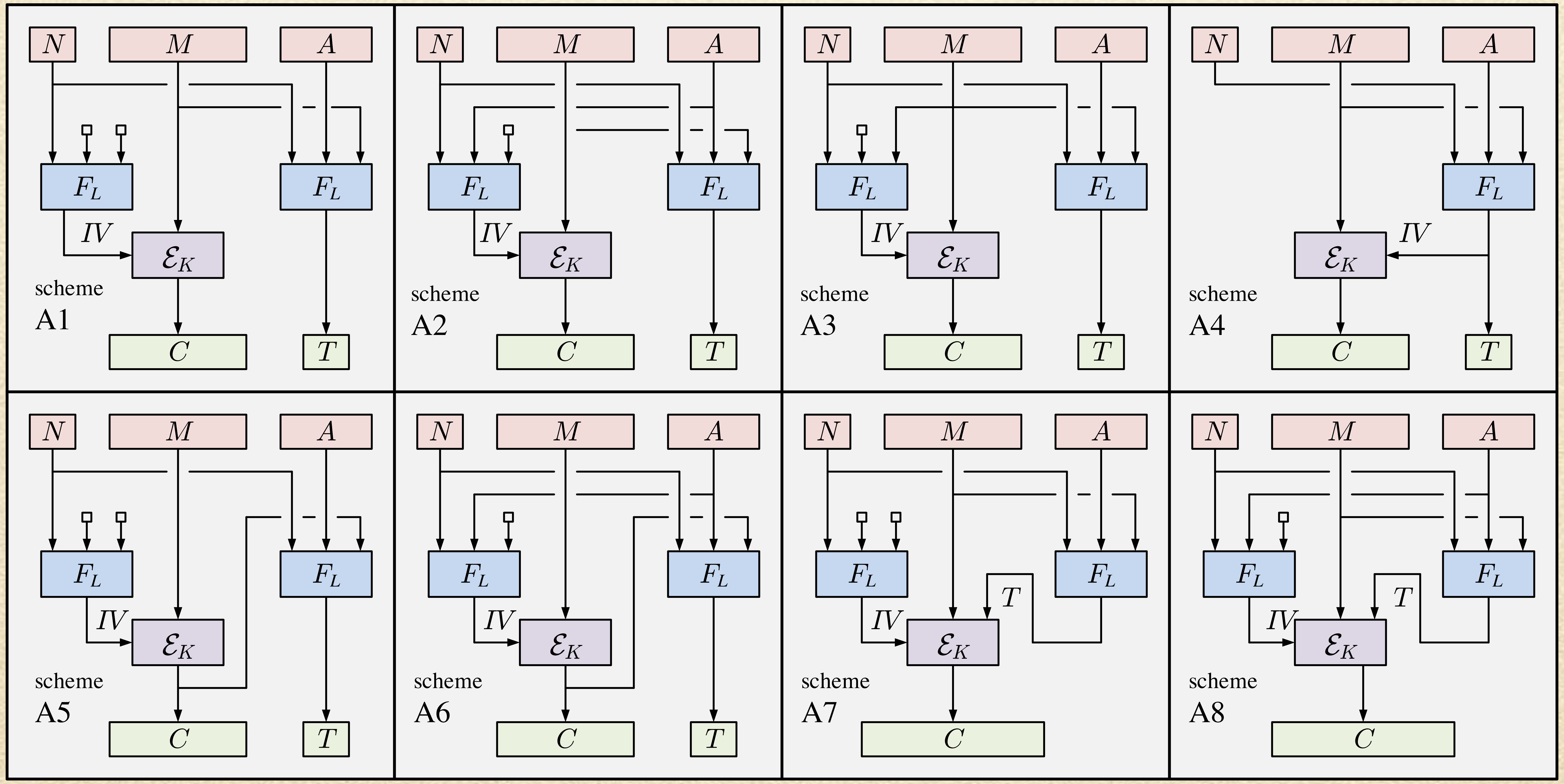


Enc-then-Mac

Mac-then-Enc

Generic Composition [NRS14]

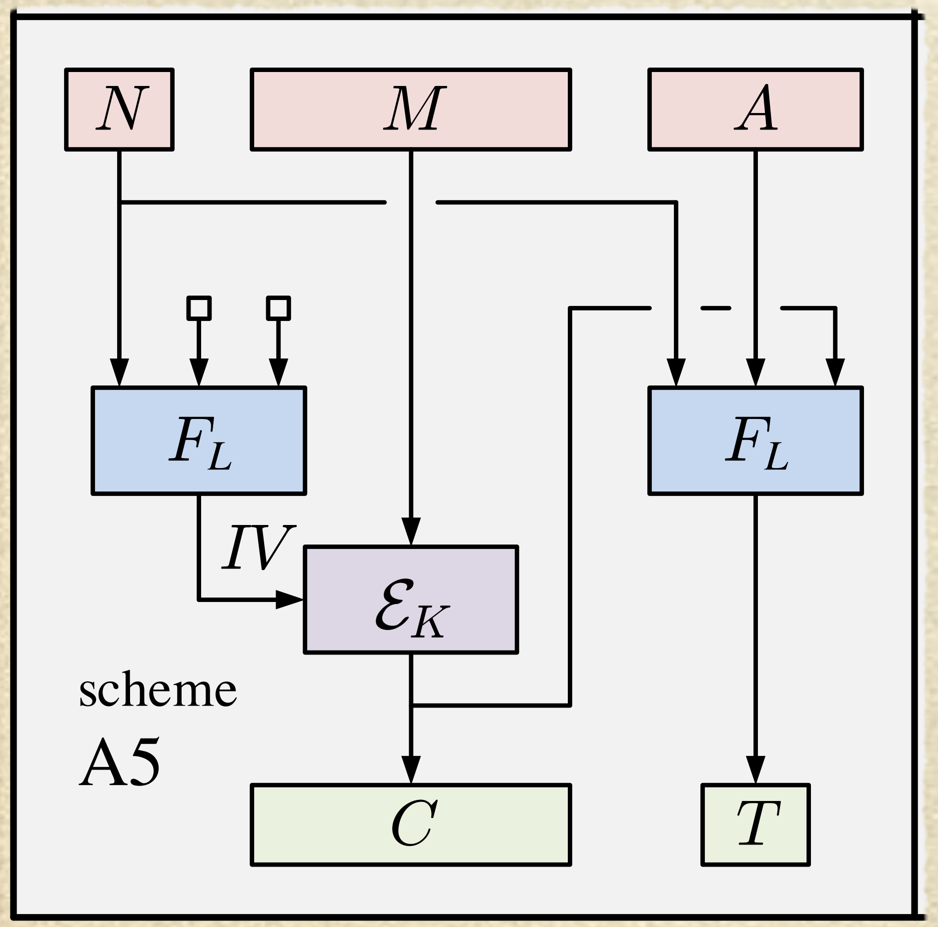
SIV



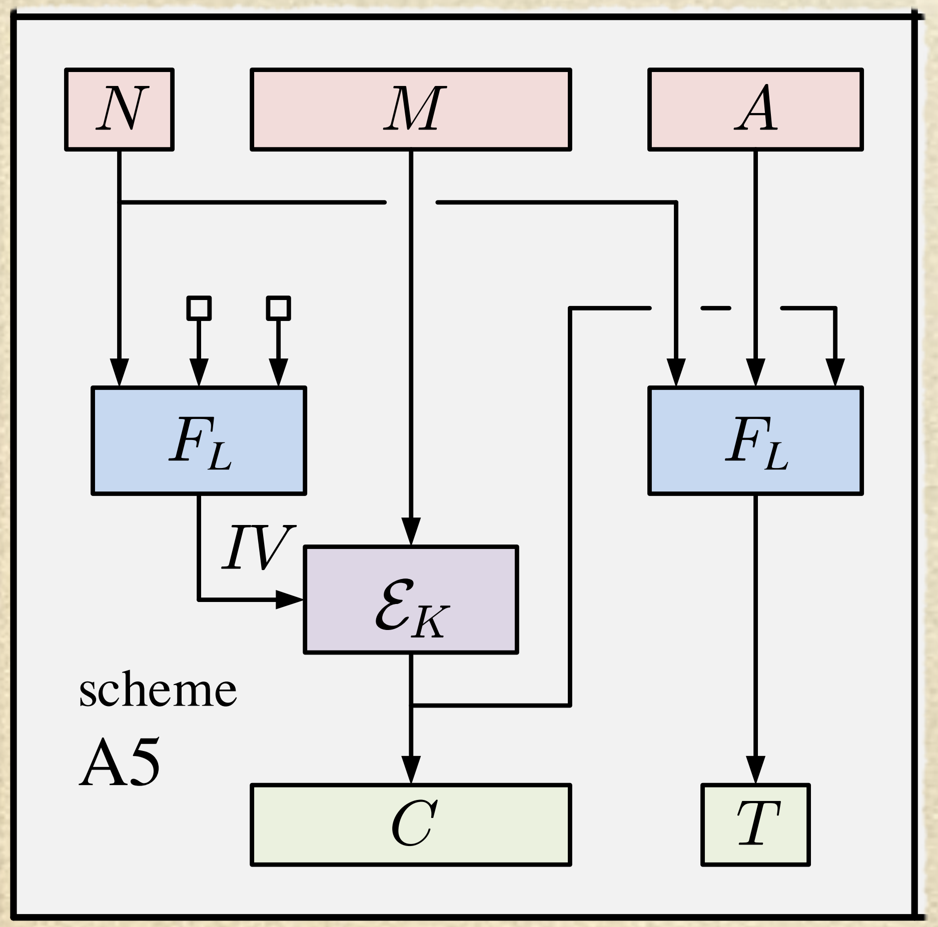
Enc-then-Mac

Mac-then-Enc

Attack on Enc-then-Mac



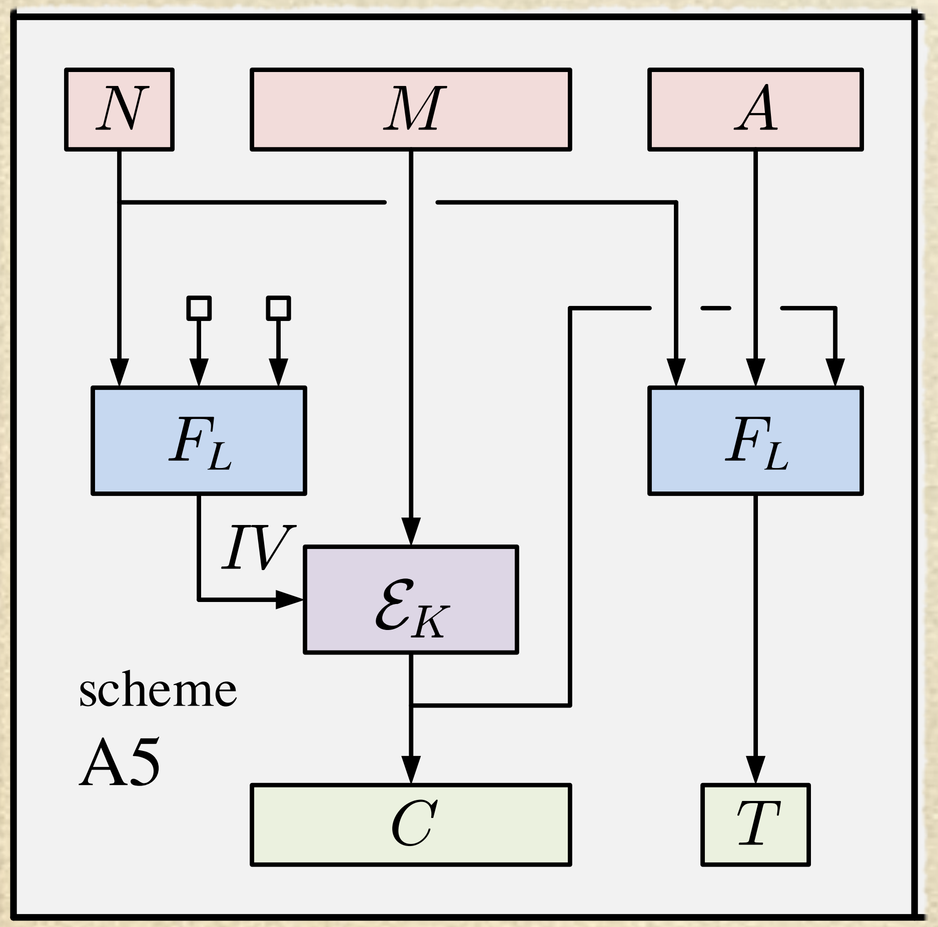
Attack on Enc-then-Mac



Construction: *Changing K does not affect T*

iEnc: *Random Injection: changing K will change T*

Attack on Enc-then-Mac



Construction: *Changing K does not affect T*
iEnc: *Random Injection: changing K will change T*

Interpretation: *Related-Key Attacks*

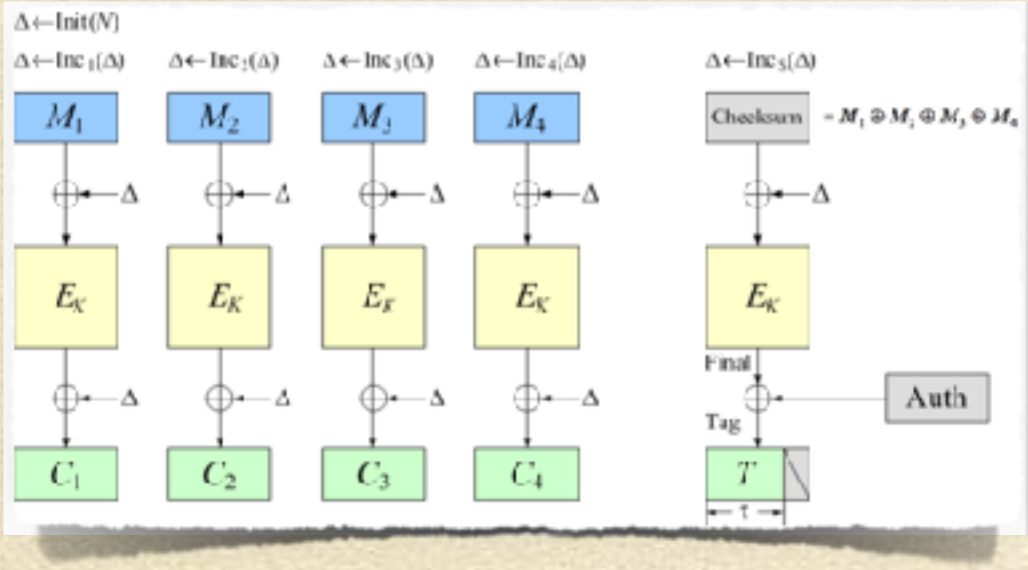
General Attacks

$\underline{\textsc{Algo. } \mathcal{AE}(K, N, A, M, \tau)}$	$\underline{\textsc{Algo. } \mathcal{AD}(K, N, A, C, \tau)}$
$(est_0, est_1) \leftarrow \mathcal{I}_e(K, N, A, M, \tau)$	$(dst_0, dst_1) \leftarrow \mathcal{I}_d(K, N, A, C, \tau)$
$(K', N', M', \tau') \leftarrow \mathcal{E}_0^{\mathcal{H}}(est_0)$	$(K', N', C', \tau') \leftarrow \mathcal{D}_0^{\mathcal{H}}(dst_0)$
$C' \leftarrow \mathcal{E}(K', N', \varepsilon, M', \tau')$	$M' \leftarrow \mathcal{D}(K', N', \varepsilon, C', \tau')$
$C \leftarrow \mathcal{E}_1^{\mathcal{H}}(C', est_1)$	$M \leftarrow \mathcal{D}_1^{\mathcal{H}}(M', dst_1)$
return C	return M

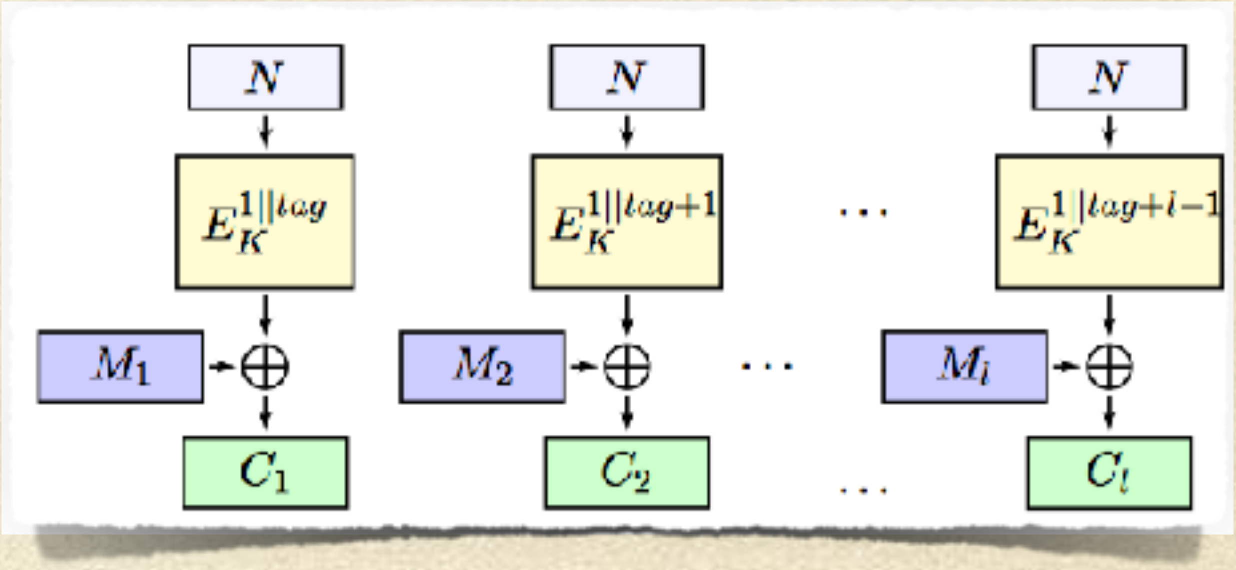
A template for generic composition.

Two types of attacks based on how information flows.

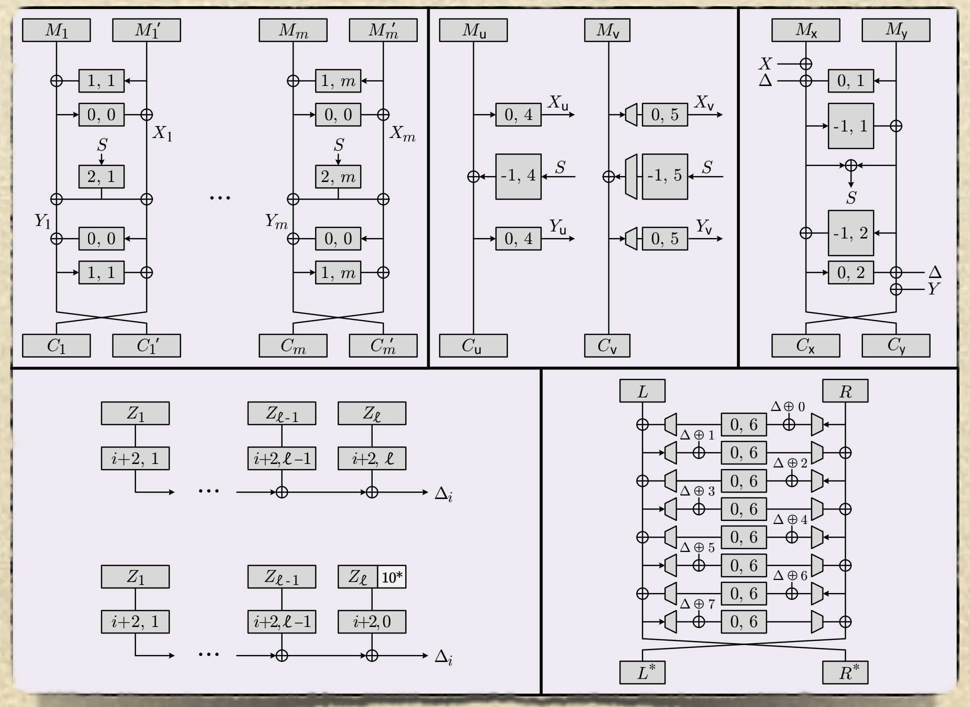
Attacks: Specifics Schemes



OCB [Rog et al.]



Deoxys [JNP15]



AEZ [HKR17]

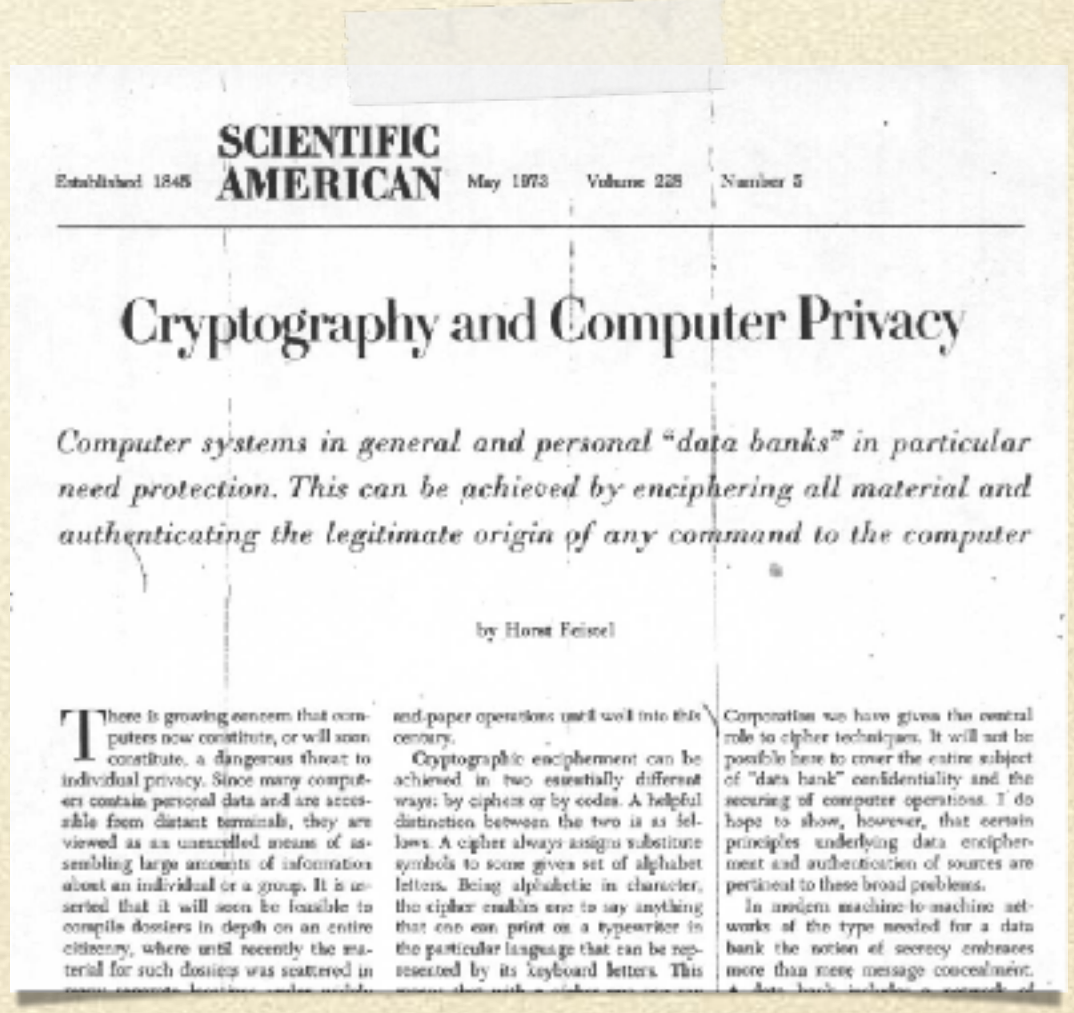
Indifferntius

.Vō porcia carhonis vticenſis tochī das lxxix ca·

So…

Any indifferentiable encryption schemes?

Feistel



Established 1845 SCIENTIFIC AMERICAN May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or a group. It is asserted that it will soon be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in

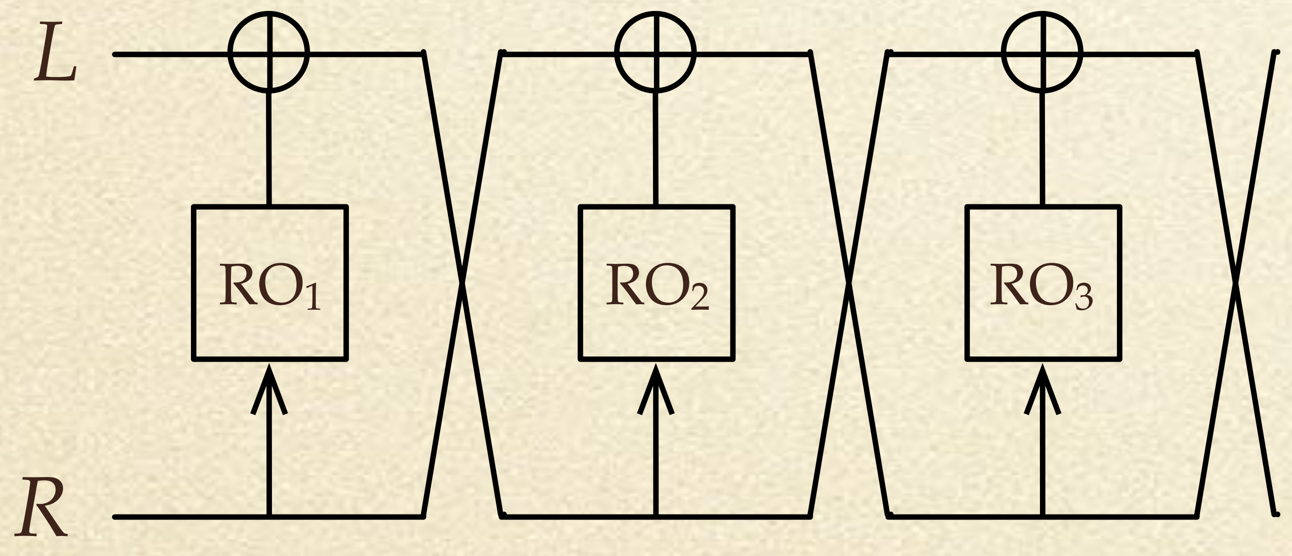
and-paper operations until well into this century.

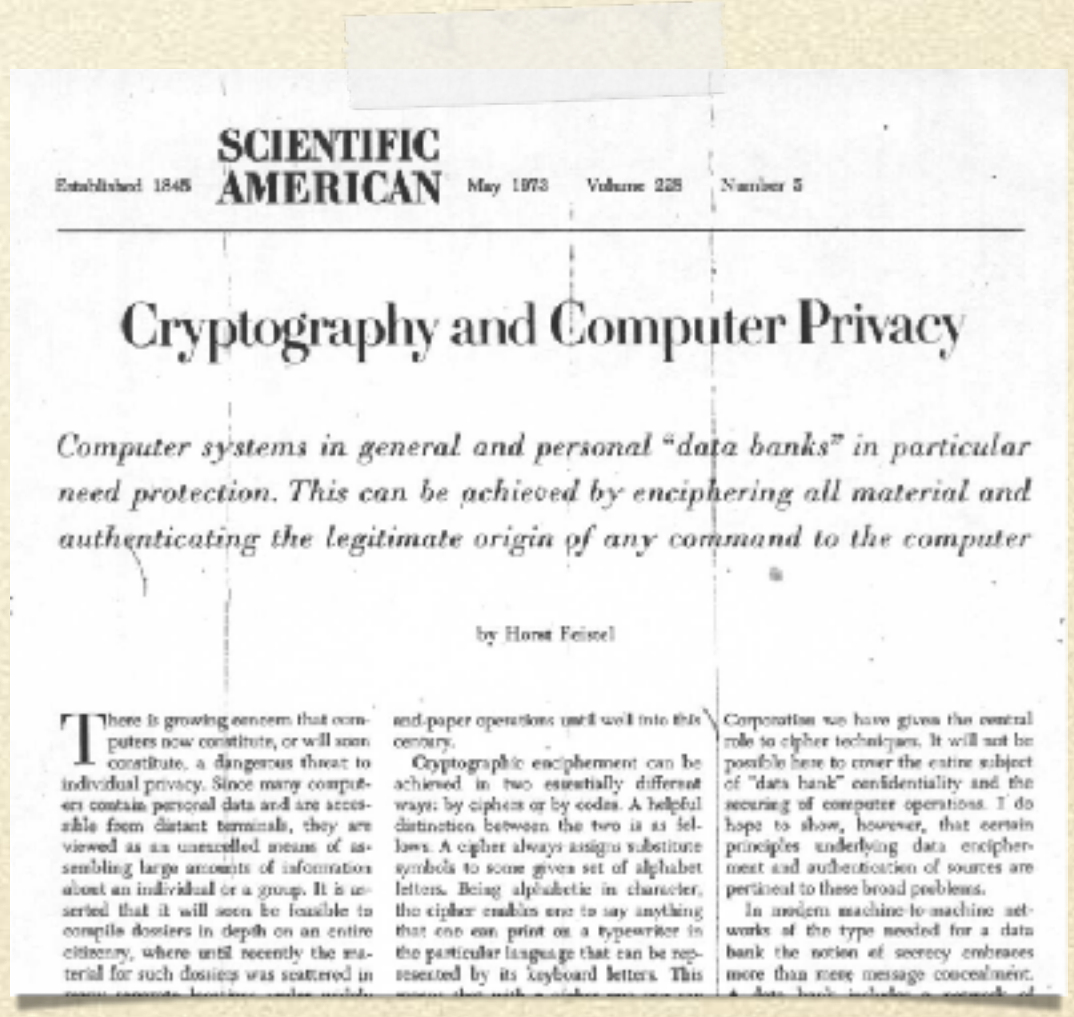
Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute symbols to some given set of alphabet letters. Being alphabetic in character, the cipher enables one to say anything that one can print on a typewriter in the particular language that can be represented by its keyboard letters. This

Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipherment and authentication of sources are pertinent to these broad problems.

In modern machine-to-machine networks of the type needed for a data bank the notion of secrecy embraces more than mere message concealment.

Feistel





Established 1845 SCIENTIFIC AMERICAN May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or a group. It is asserted that it will soon be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in

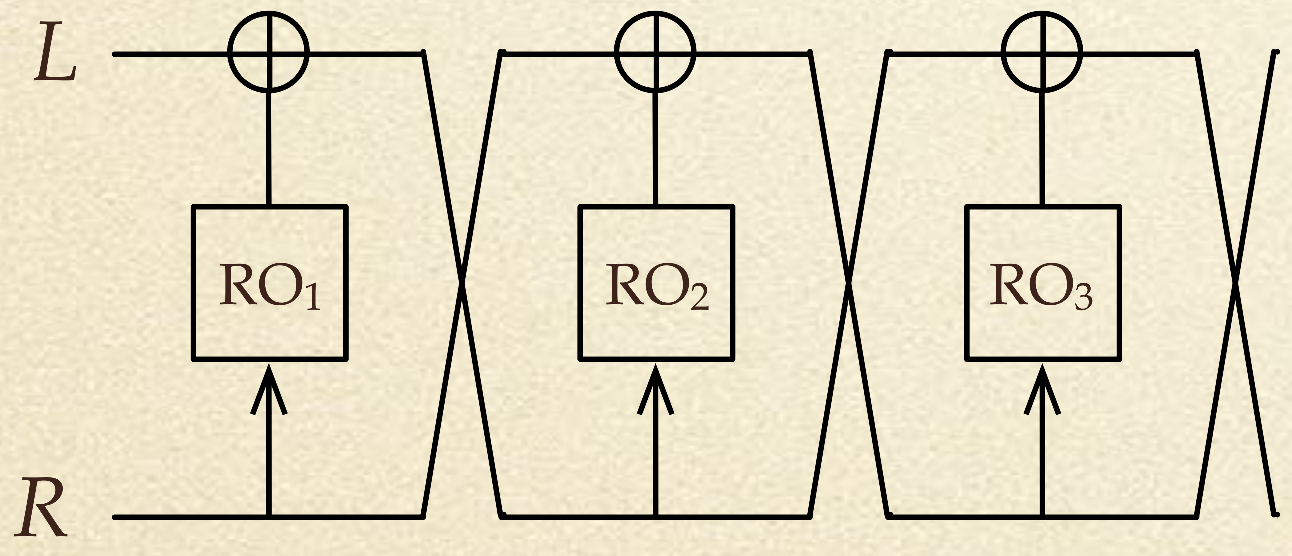
and-paper operations until well into this century.

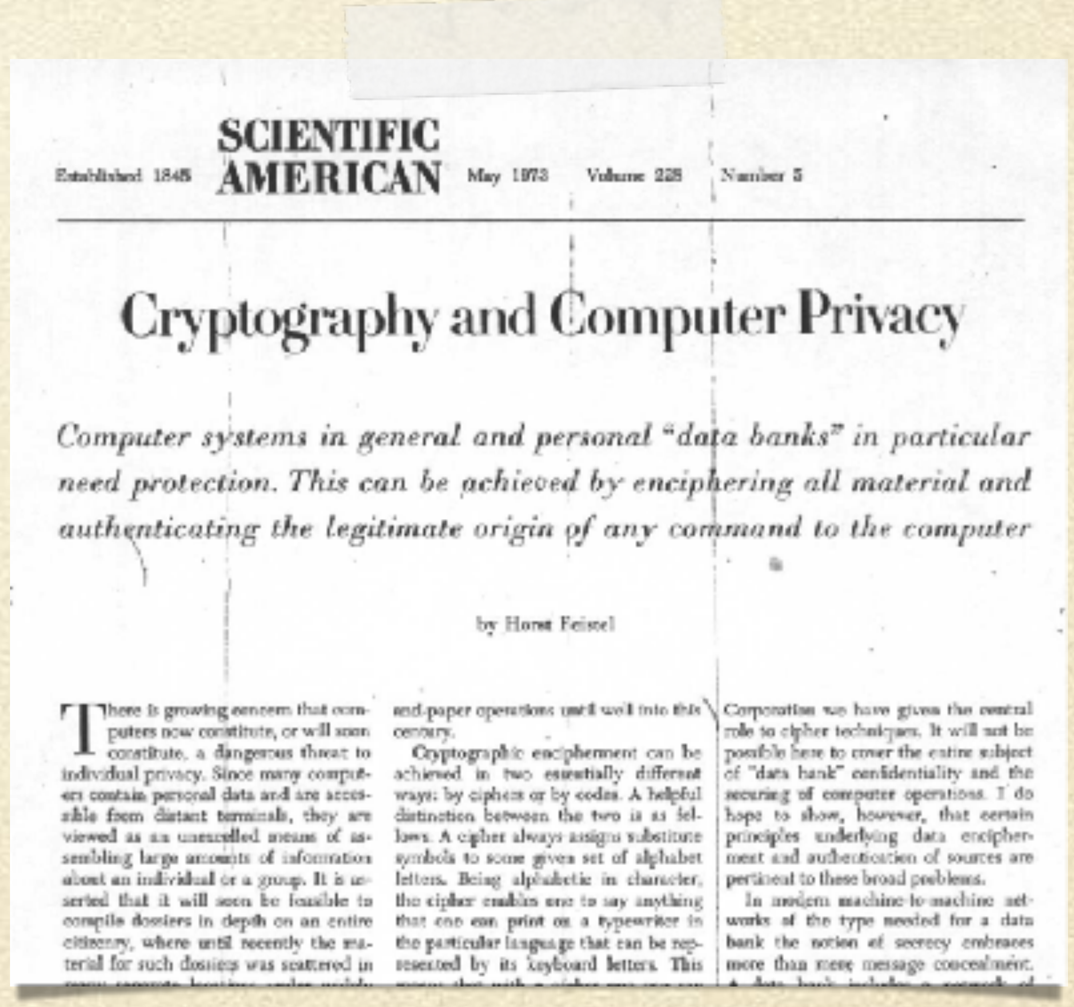
Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute symbols to some given set of alphabet letters. Being alphabetic in character, the cipher enables one to say anything that one can print on a typewriter in the particular language that can be represented by its keyboard letters. This

Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipherment and authentication of sources are pertinent to these broad problems.

In modern machine-to-machine networks of the type needed for a data bank the notion of secrecy embraces more than mere message concealment.

Feistel





Established 1845 **SCIENTIFIC AMERICAN** May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or a group. It is asserted that it will soon be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in

and-paper operations until well into this century.

Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute symbols to some given set of alphabet letters. Being alphabetic in character, the cipher enables one to say anything that one can print on a typewriter in the particular language that can be represented by its keyboard letters. This

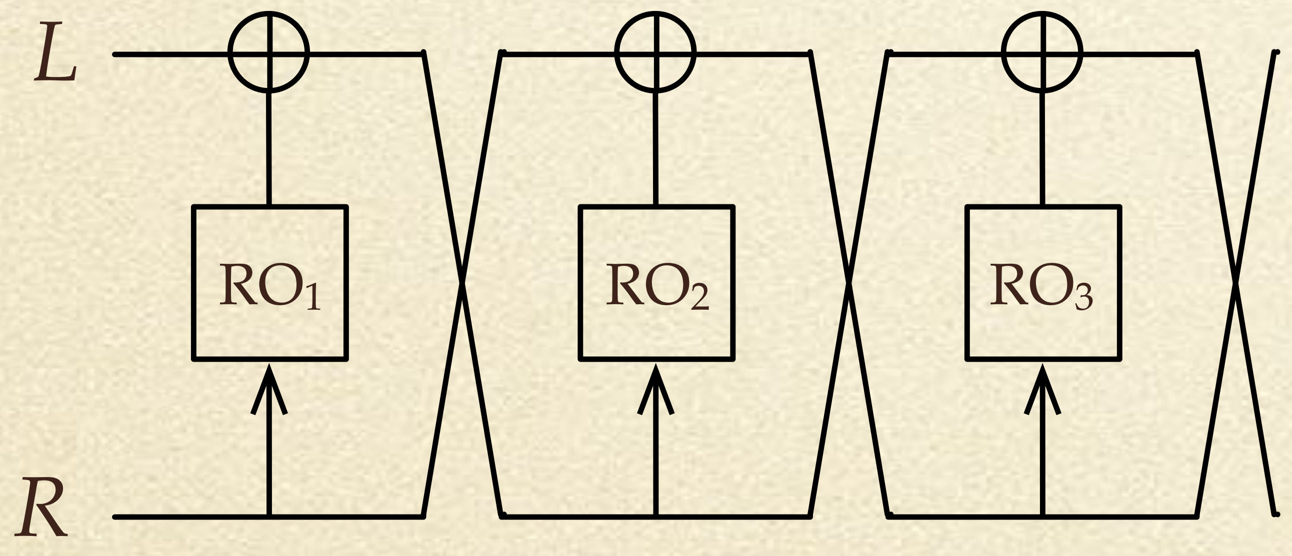
Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipherment and authentication of sources are pertinent to these broad problems.

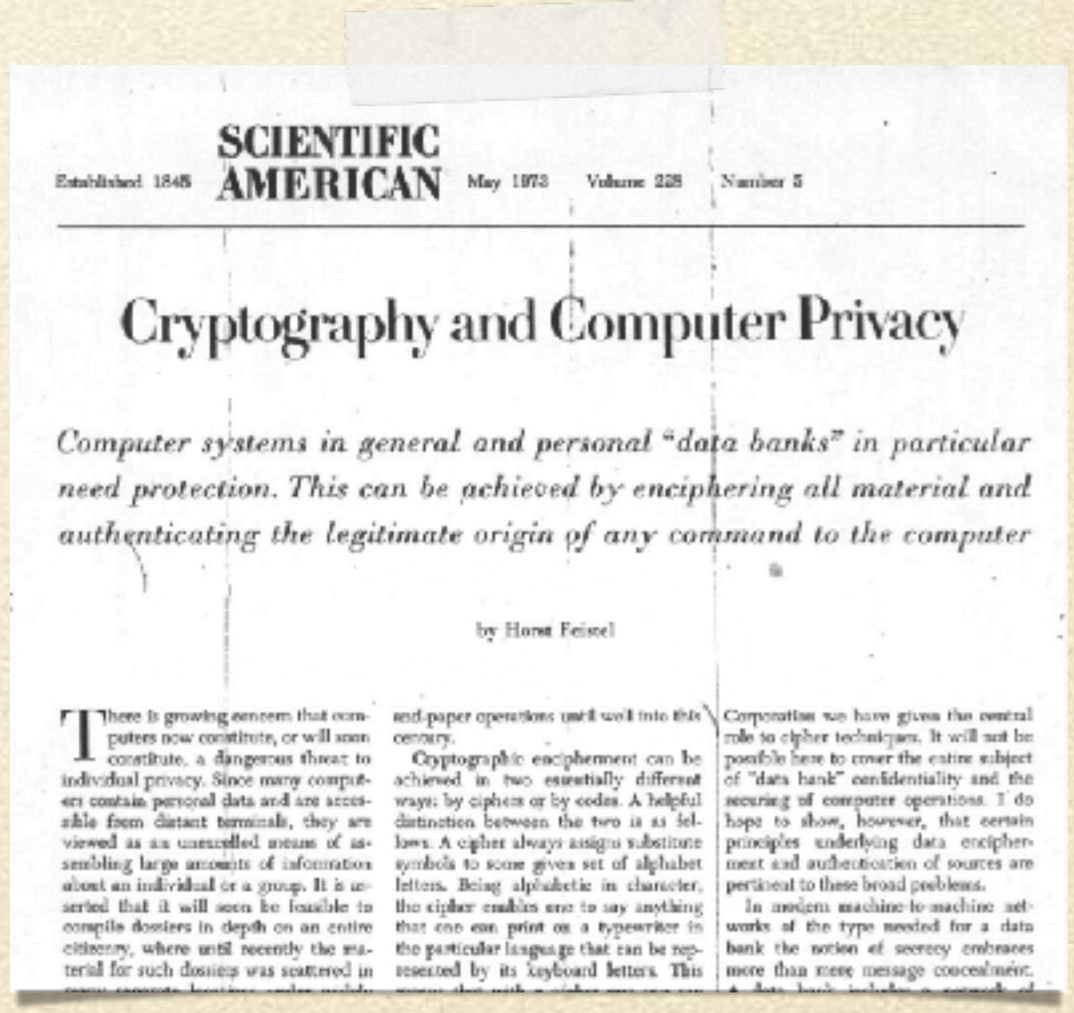
In modern machine-to-machine networks of the type needed for a data bank the notion of secrecy embraces more than mere message concealment.

1	2	3	4	5	6	7	8	9	10	11	12	13	14

Permutation

Feistel





Established 1845 SCIENTIFIC AMERICAN May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or a group. It is asserted that it will soon be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in

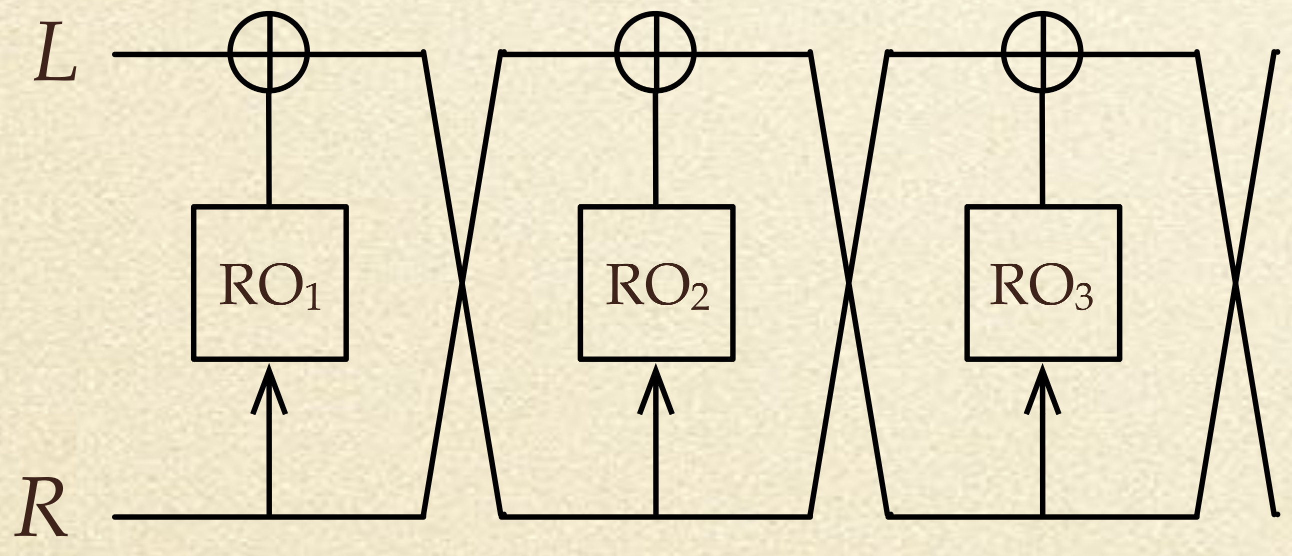
and-paper operations until well into this century.

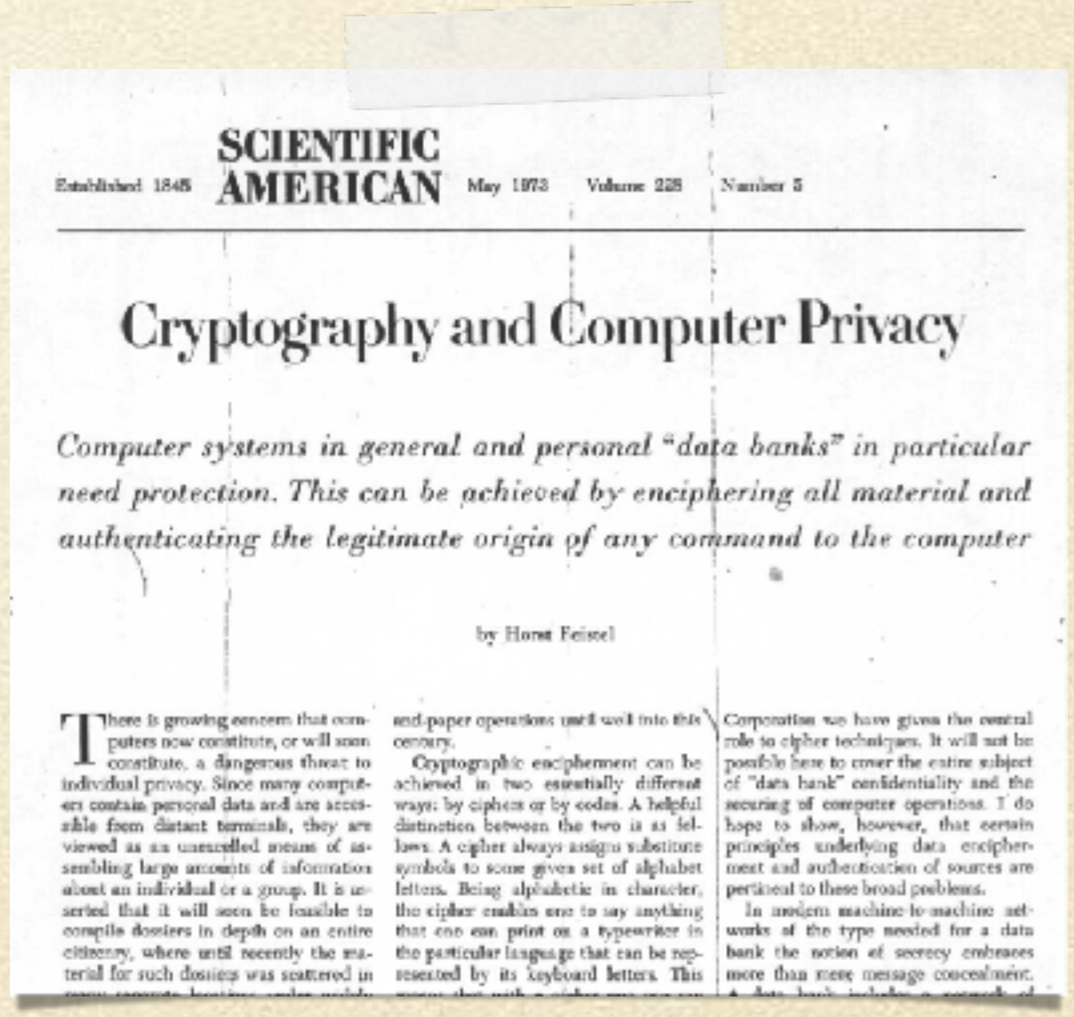
Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute symbols to some given set of alphabet letters. Being alphabetic in character, the cipher enables one to say anything that one can print on a typewriter in the particular language that can be represented by its keyboard letters. This

Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipherment and authentication of sources are pertinent to these broad problems.

In modern machine-to-machine networks of the type needed for a data bank the notion of secrecy embraces more than mere message concealment.

Feistel





SCIENTIFIC AMERICAN

Established 1845 May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or a group. It is asserted that it will soon be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in

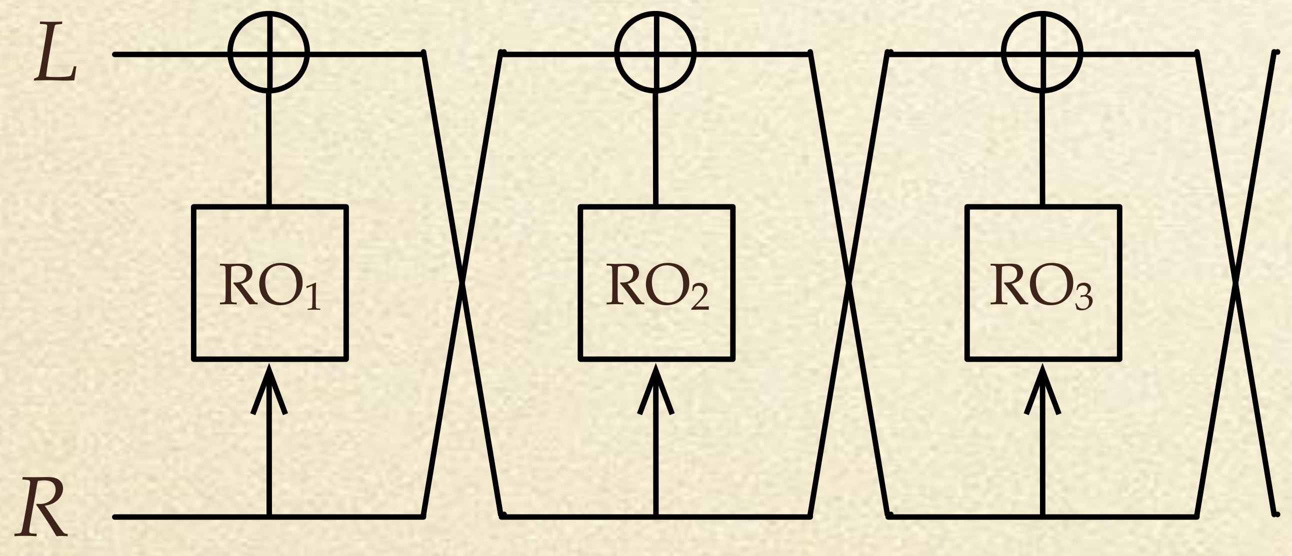
and-paper operations until well into this century.

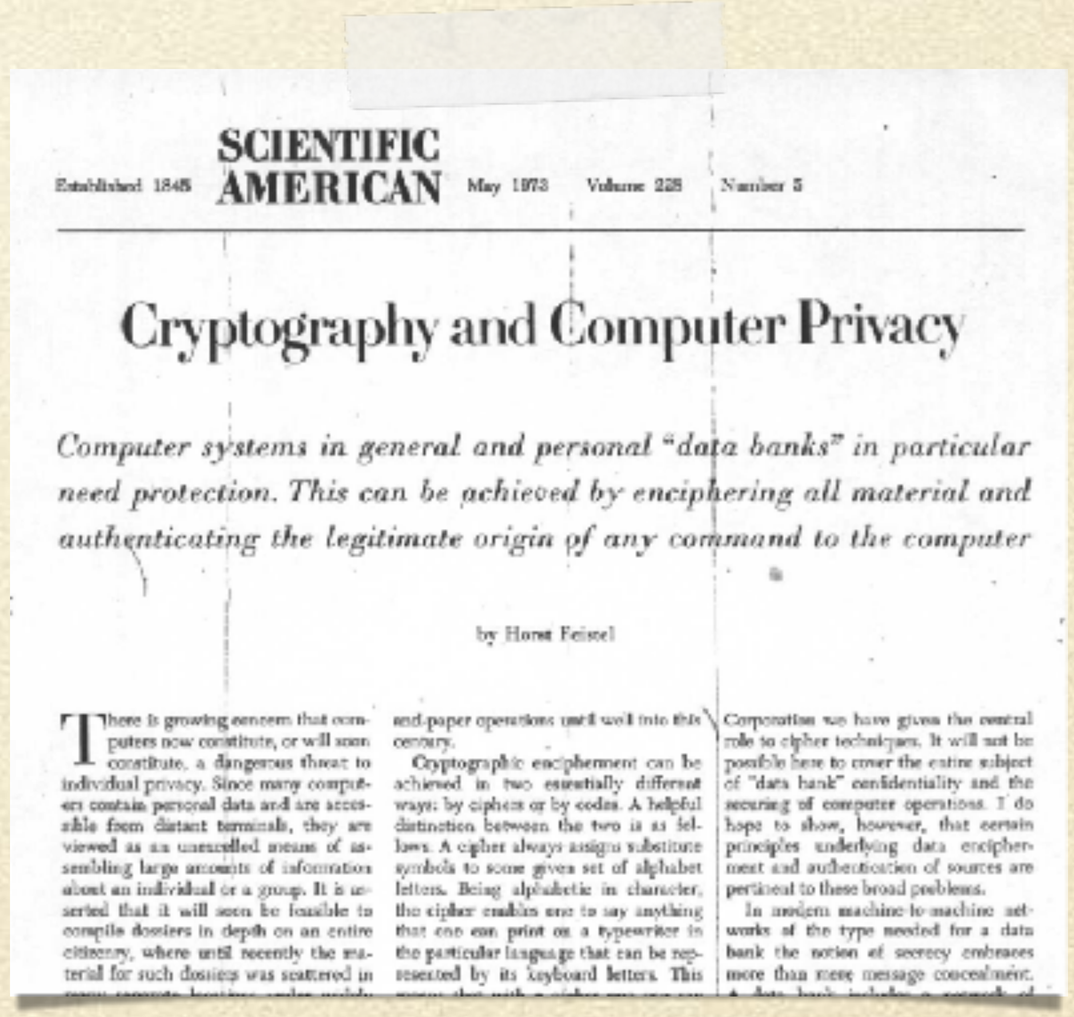
Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute symbols to some given set of alphabet letters. Being alphabetic in character, the cipher enables one to say anything that one can print on a typewriter in the particular language that can be represented by its keyboard letters. This

Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipherment and authentication of sources are pertinent to these broad problems.

In modern machine-to-machine networks of the type needed for a data bank the notion of secrecy embraces more than mere message concealment.

Feistel





Established 1845 SCIENTIFIC AMERICAN May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or a group. It is asserted that it will soon be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in

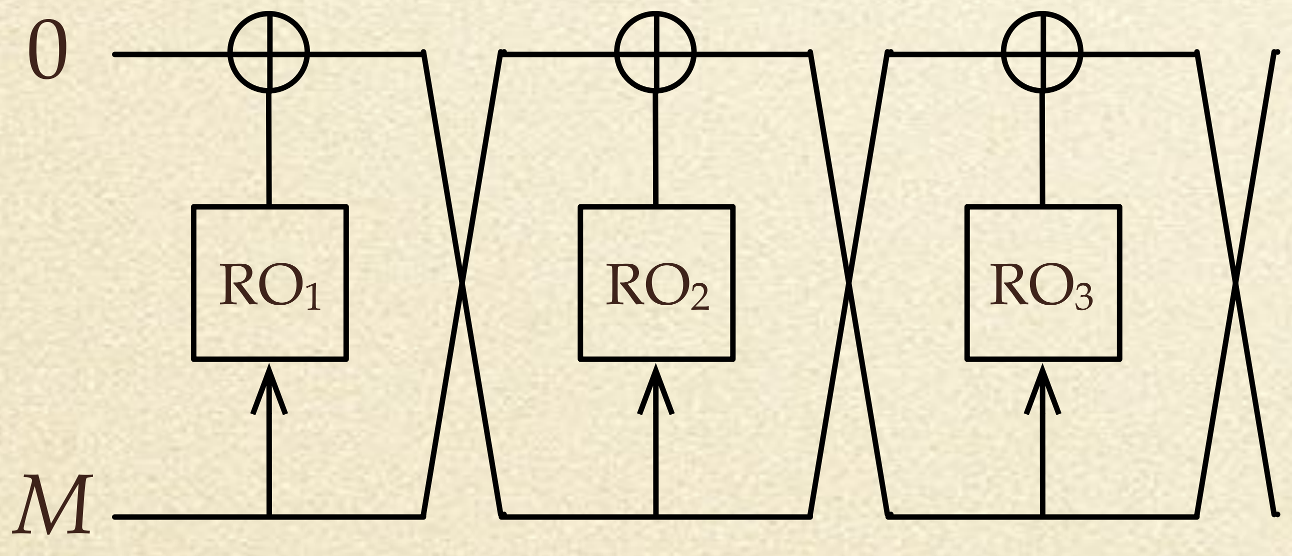
and-paper operations until well into this century.

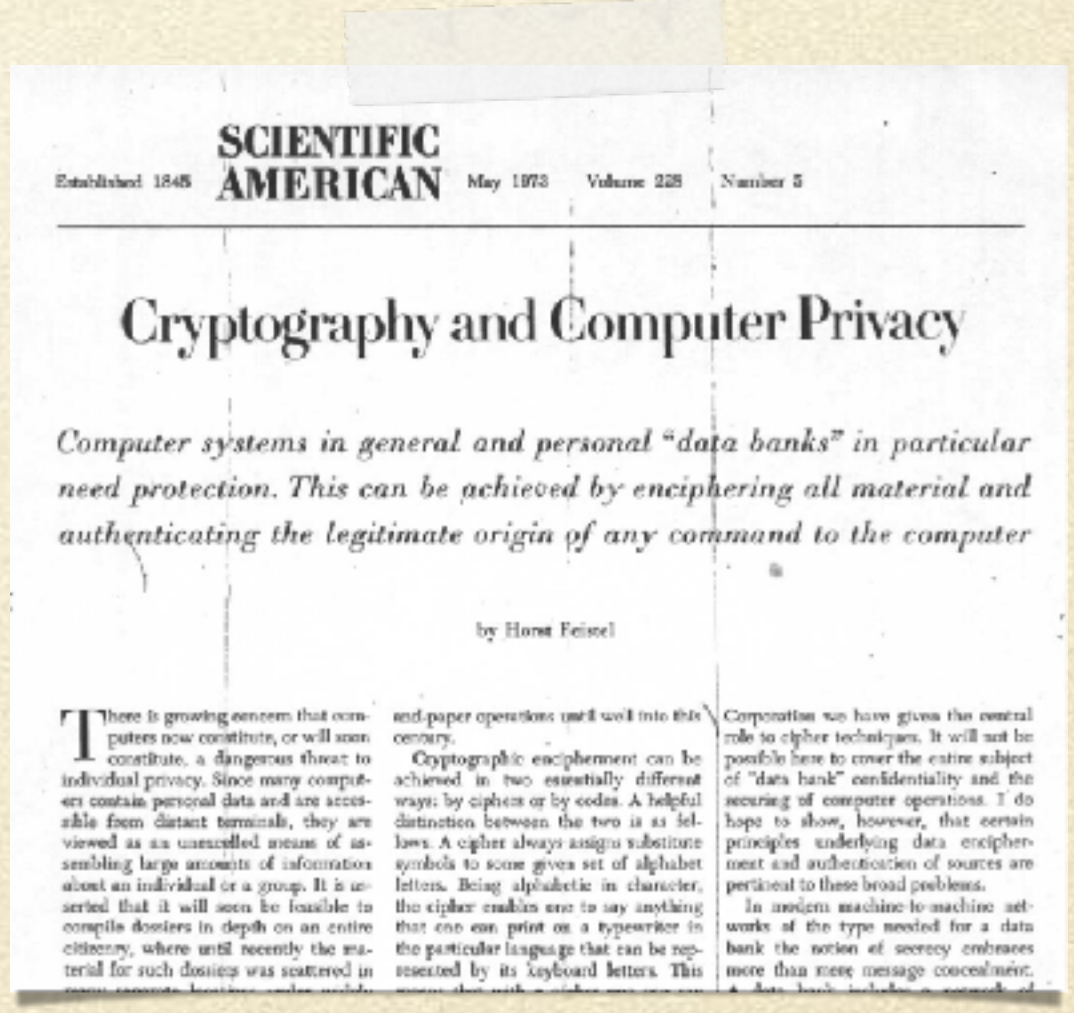
Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute symbols to some given set of alphabet letters. Being alphabetic in character, the cipher enables one to say anything that one can print on a typewriter in the particular language that can be represented by its keyboard letters. This

Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipherment and authentication of sources are pertinent to these broad problems.

In modern machine-to-machine networks of the type needed for a data bank the notion of secrecy embraces more than mere message concealment.

Feistel





Established 1845 SCIENTIFIC AMERICAN May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or a group. It is asserted that it will soon be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in

and-paper operations until well into this century.

Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute symbols to some given set of alphabet letters. Being alphabetic in character, the cipher enables one to say anything that one can print on a typewriter in the particular language that can be represented by its keyboard letters. This

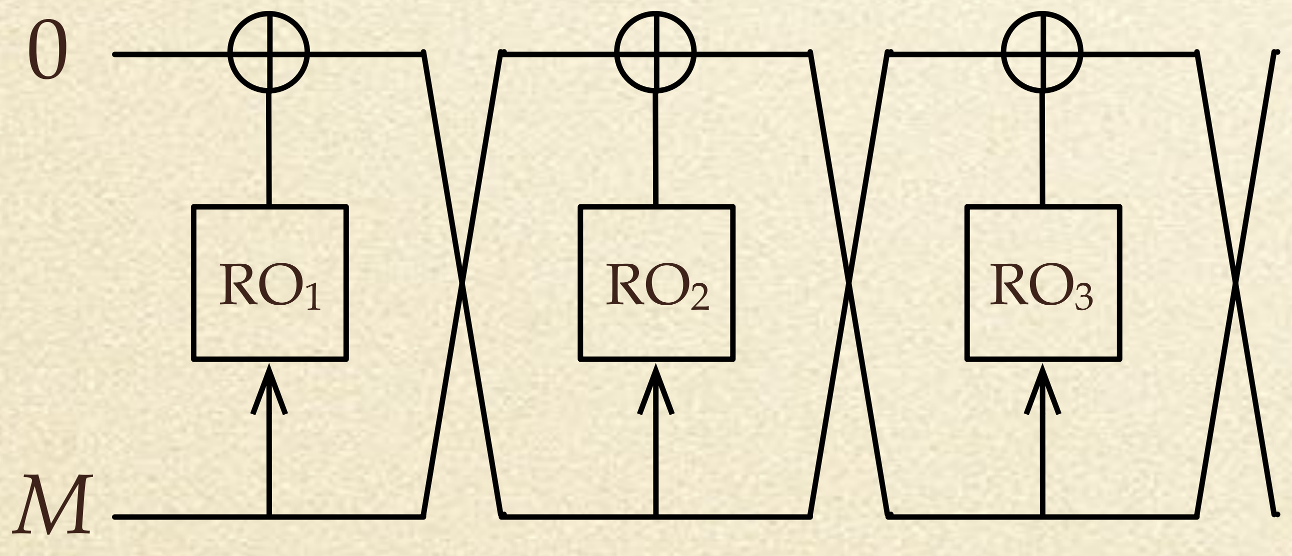
Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipherment and authentication of sources are pertinent to these broad problems.

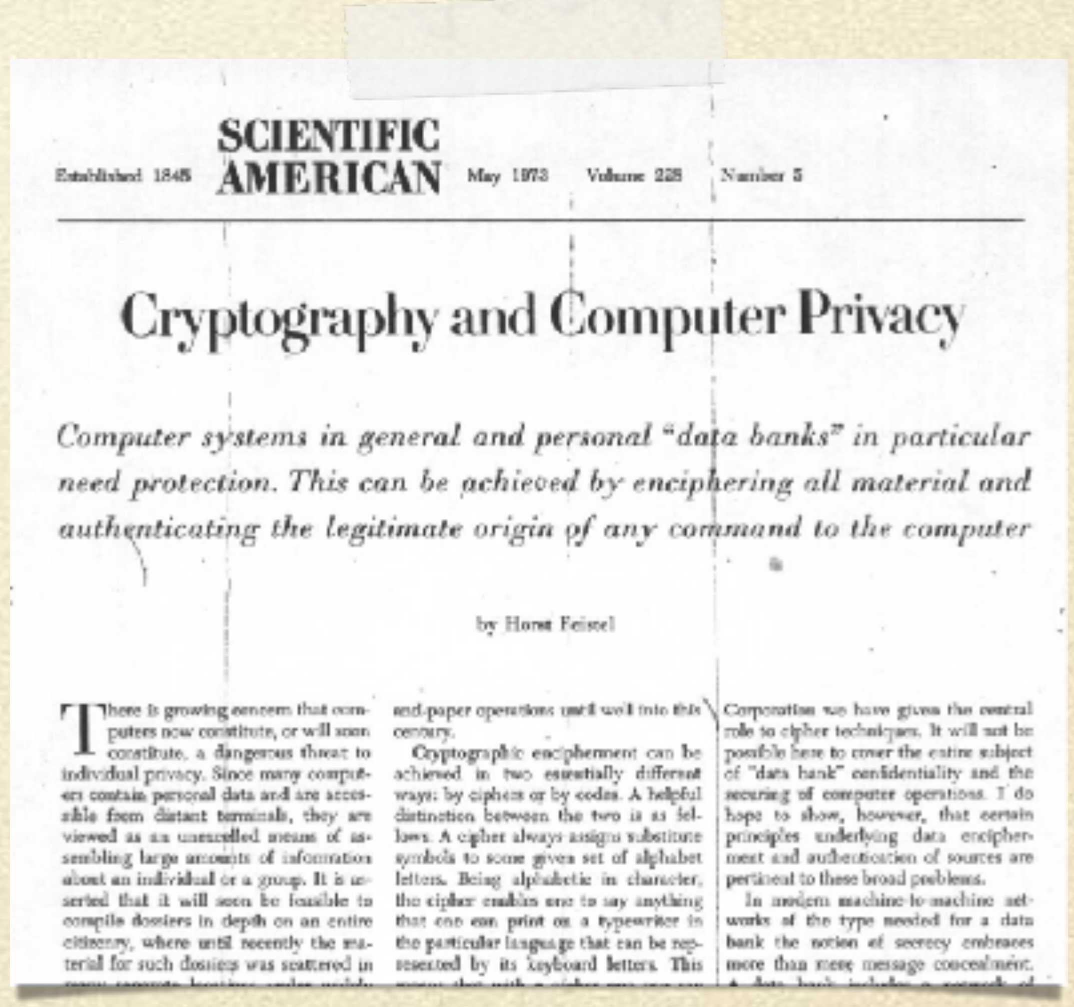
In modern machine-to-machine networks of the type needed for a data bank the notion of secrecy embraces more than mere message concealment.

1 2 3 4 5 6 7 8 9 10 11 12 13 14

Permutation

Feistel





SCIENTIFIC AMERICAN

Established 1845 May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or a group. It is asserted that it will soon be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in

and-paper operations until well into this century.

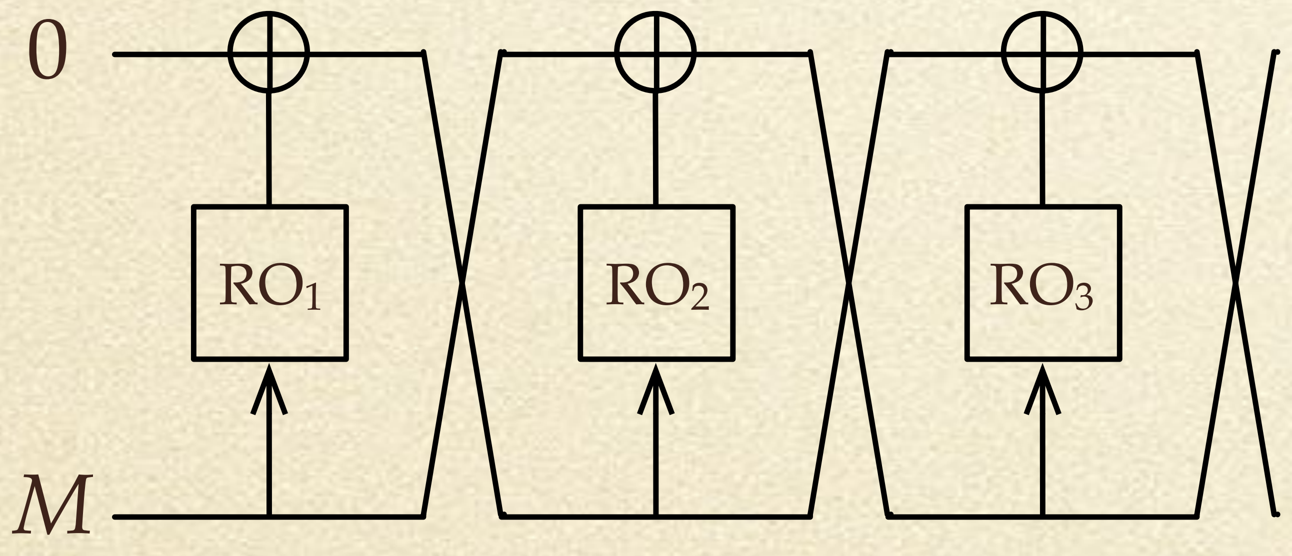
Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute symbols to some given set of alphabet letters. Being alphabetic in character, the cipher enables one to say anything that one can print on a typewriter in the particular language that can be represented by its keyboard letters. This

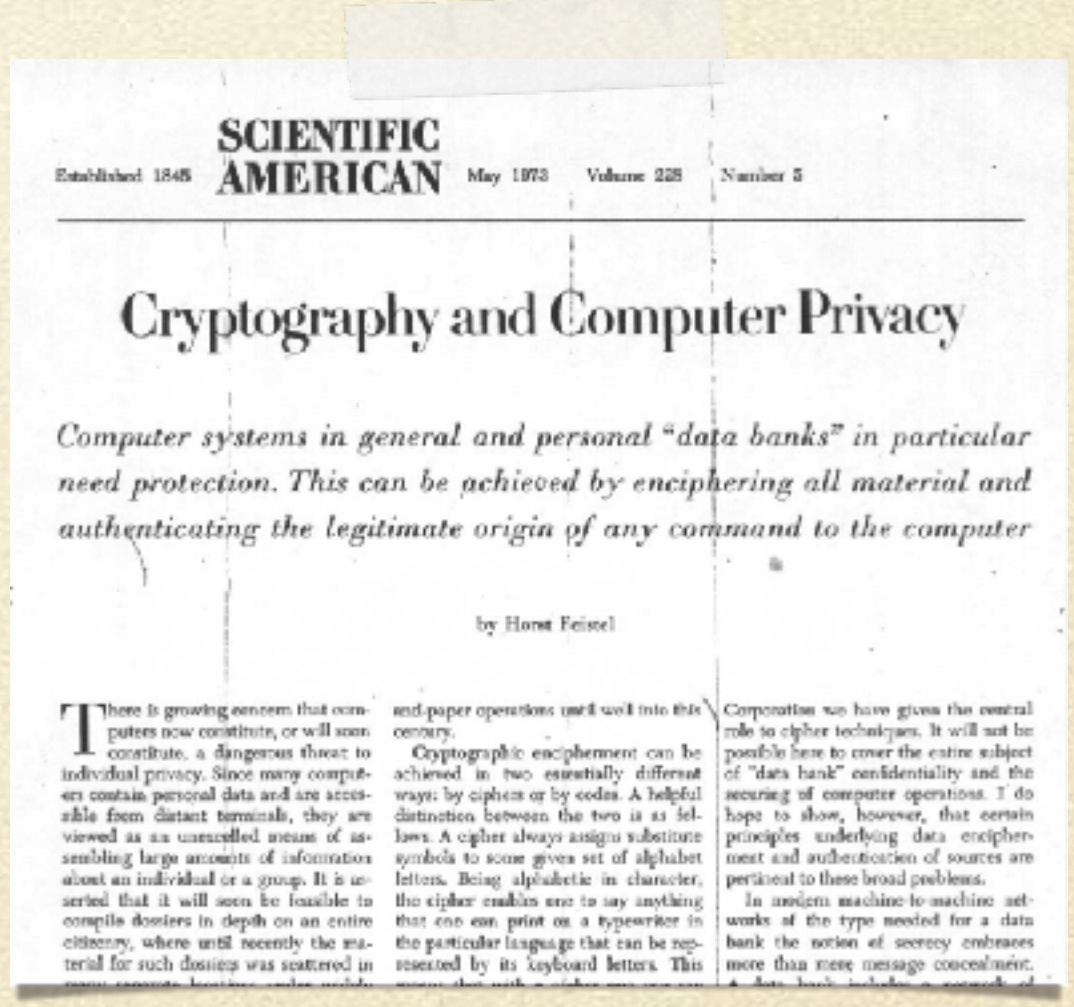
Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipherment and authentication of sources are pertinent to these broad problems.

In modern machine-to-machine networks of the type needed for a data bank the notion of secrecy embraces more than mere message concealment.

Theorem: *3 rounds of Feistel are necessary and sufficient to build a random injection.*

Feistel





Established 1845 **SCIENTIFIC AMERICAN** May 1973 Volume 228 Number 5

Cryptography and Computer Privacy

Computer systems in general and personal "data banks" in particular need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer

by Horst Feistel

There is growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or a group. It is asserted that it will soon be feasible to compile dossiers in depth on an entire citizenry, where until recently the material for such dossiers was scattered in [illegible] and-paper operations until well into this century.

Cryptographic encipherment can be achieved in two essentially different ways: by ciphers or by codes. A helpful distinction between the two is as follows. A cipher always assigns substitute symbols to some given set of alphabet letters. Being alphabetic in character, the cipher enables one to say anything that one can print on a typewriter in the particular language that can be represented by its keyboard letters. This [illegible] Corporation we have given the central role to cipher techniques. It will not be possible here to cover the entire subject of "data bank" confidentiality and the securing of computer operations. I do hope to show, however, that certain principles underlying data encipherment and authentication of sources are pertinent to these broad problems.

In modern machine-to-machine networks of the type needed for a data bank the notion of secrecy embraces more than mere message concealment. [illegible]

***Theorem**: 3 rounds of Feistel are necessary and sufficient to build a random injection.*

Injection

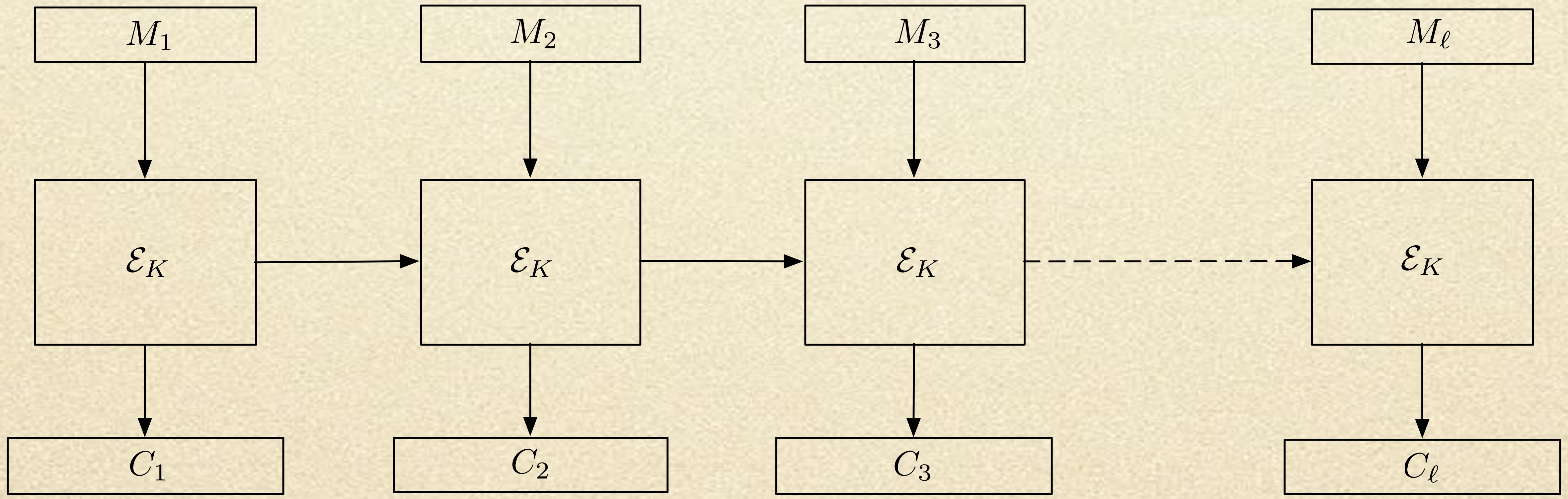
1 2 3 4 5 6 7 8 9 10 11 12 13 14

1 2 3 4 5 6 7 8 9 10 11 12 13 14

Permutation

Online Encryption

Some applications need to process messages "on the fly":



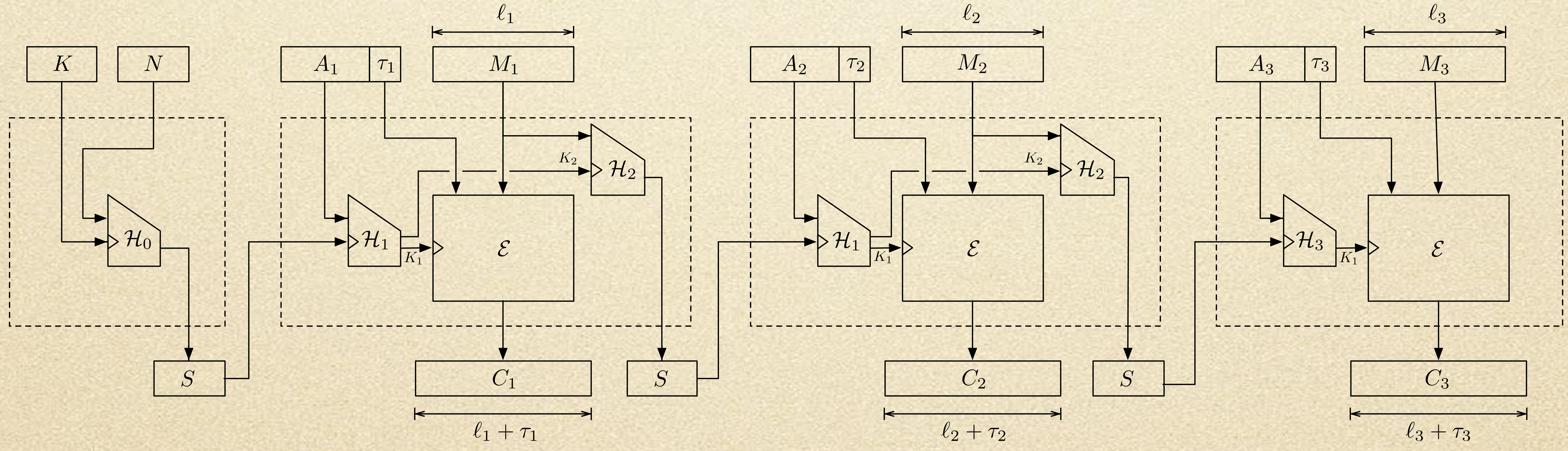
*Leads to: A definition of **online** random keyed injections.*

Turning It On

Theorem: *Chaining an AEAD up indifferentiability turns it on.*

Turning It On

Theorem: *Chaining an AEAD up indifferentiability turns it on.*



Efficiency Lower Bound

Theorem: *Any indifferentiable construction of a wn-bit random injection from an n-bit permutation must place at least $2w$-2 queries.*

Efficiency Lower Bound

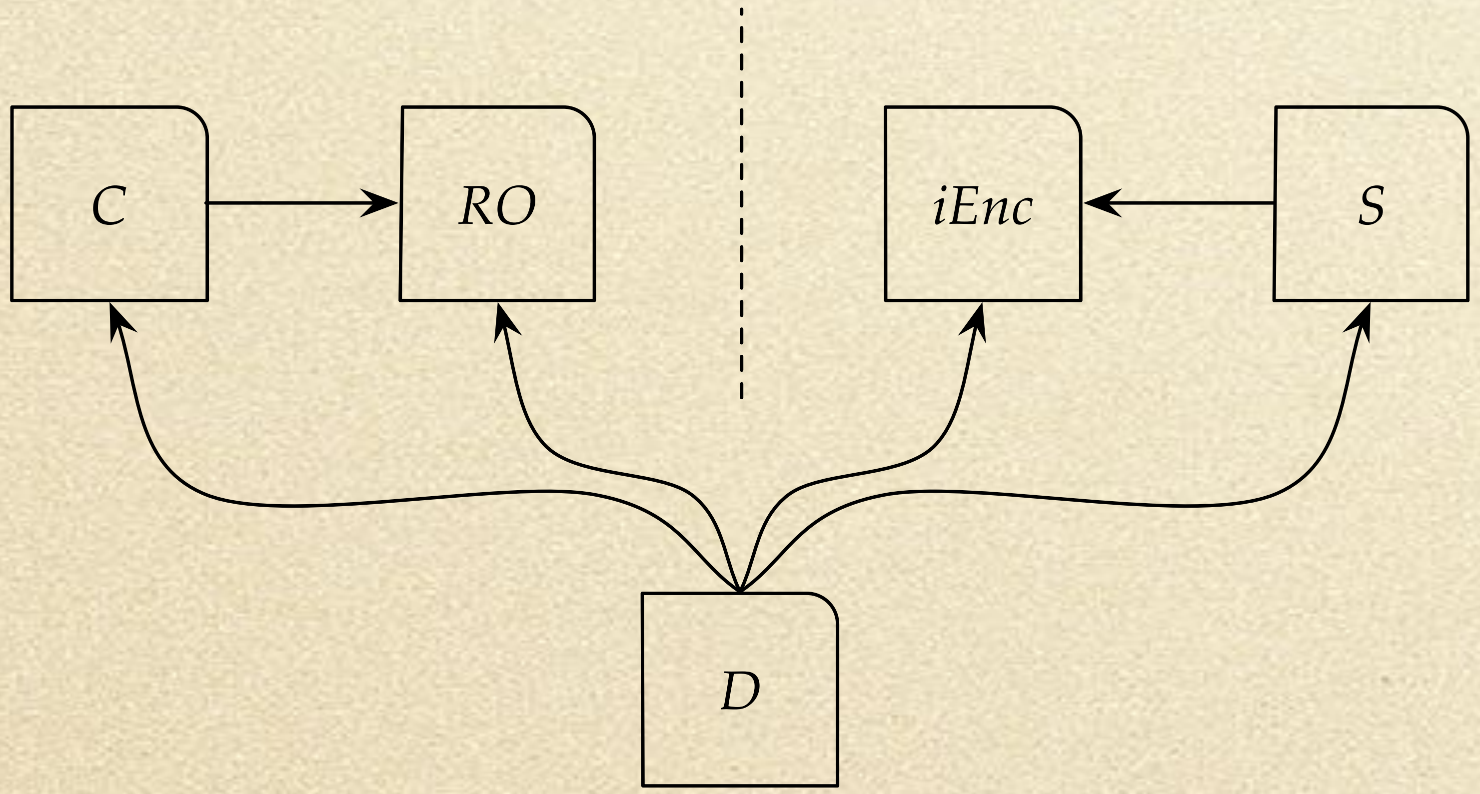
Theorem: *Any indifferentiable construction of a wn-bit random injection from an n-bit permutation must place at least $2w$-2 queries.*

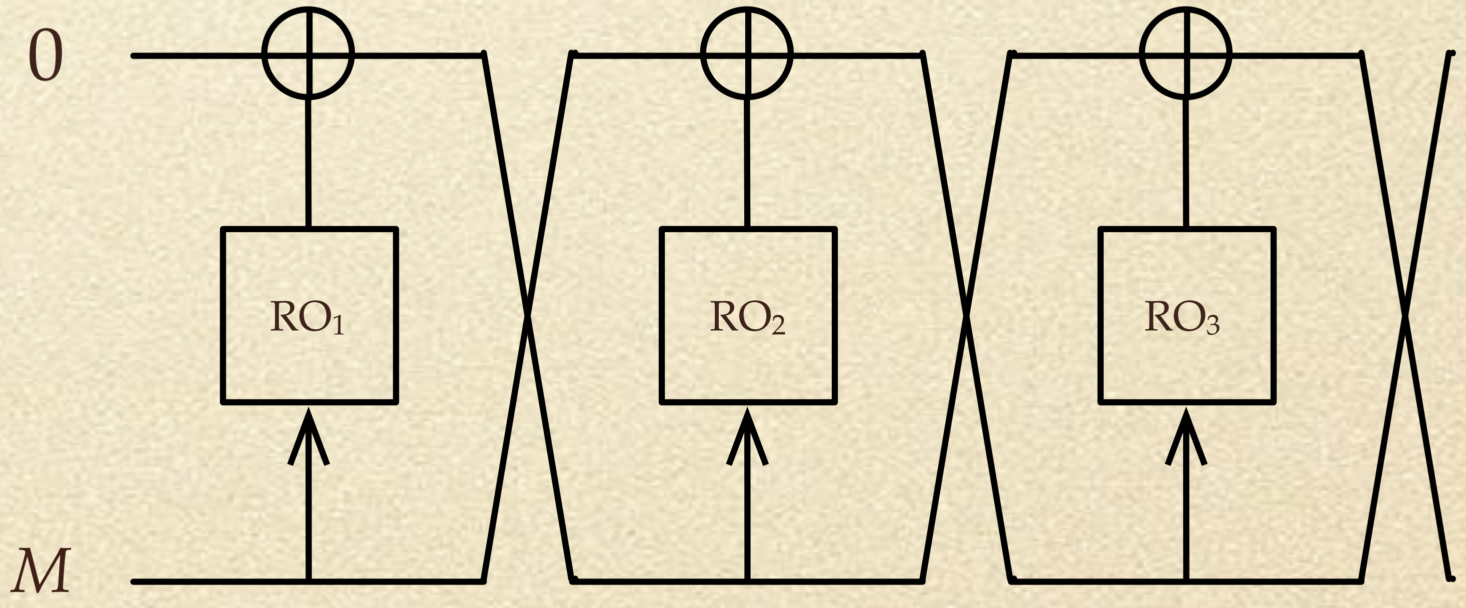
Lower/upper bounds remain open for:

$$\rho := \frac{\#\text{ blocks}}{\#\text{ queries}} \in [2,3)\ .$$

Summary

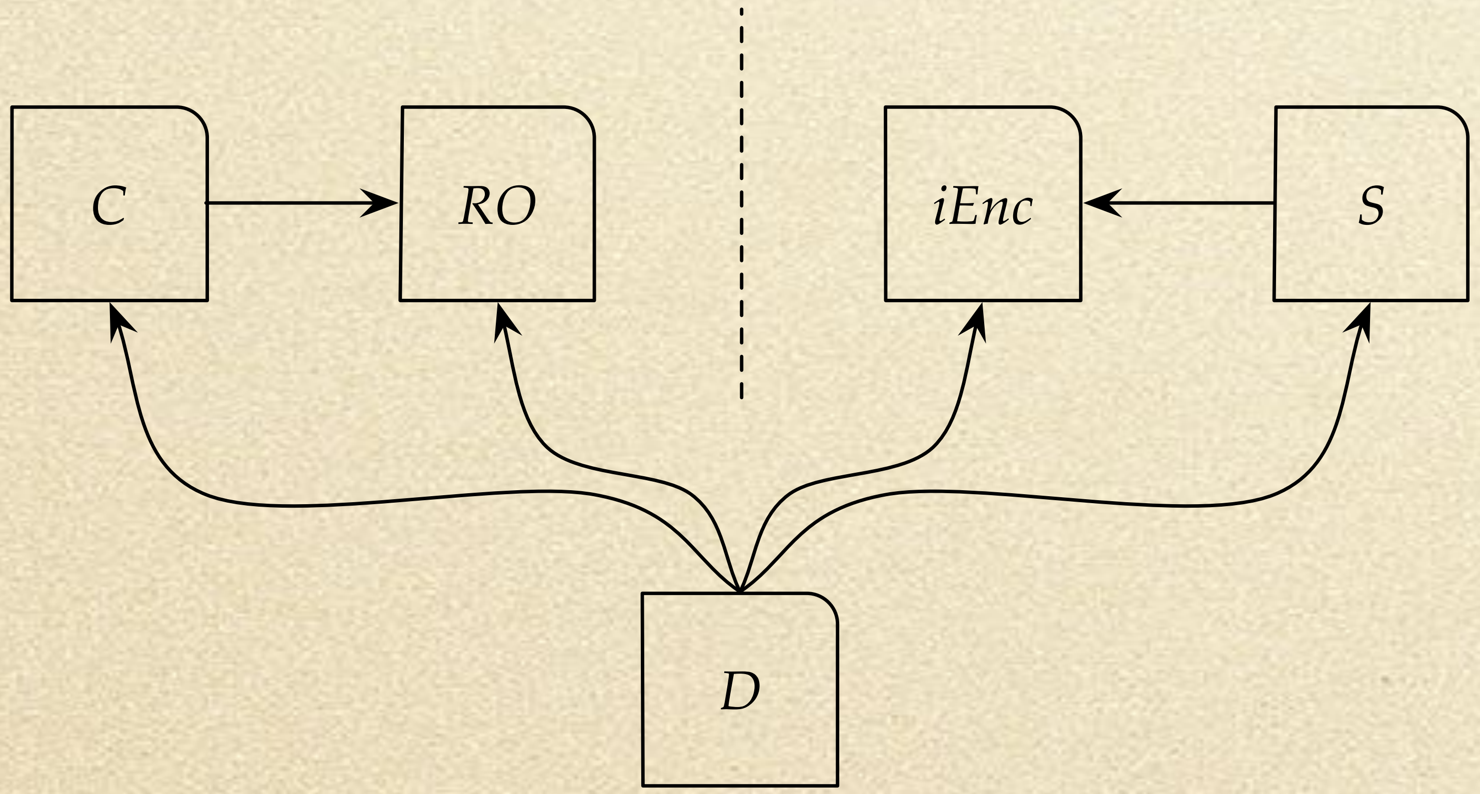
New view of AE as a random keyed injection;
Implies security in many adversarial environments.

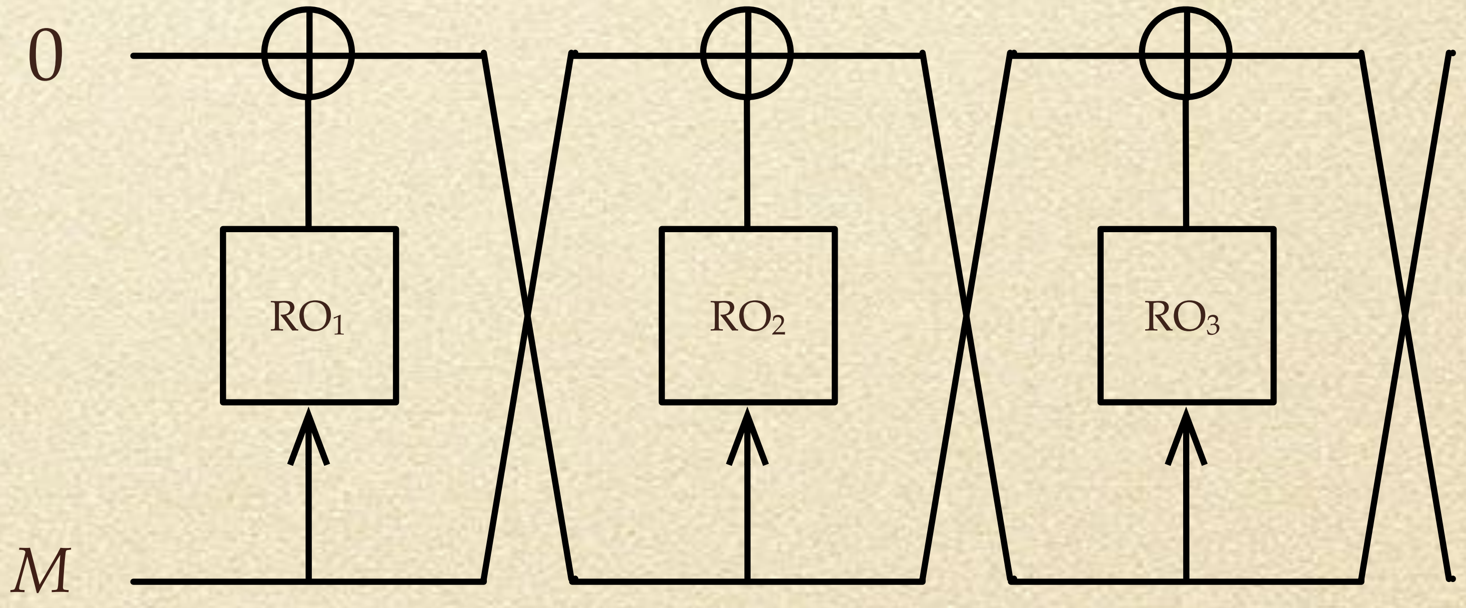




Summary

New view of AE as a random keyed injection;
Implies security in many adversarial environments.





Thank you.