ALGORITMI E PROTOCOLLI CRITTOGRAFICI PER L'ANALISI DEI DATI

Summer School **Professione Ricercatore** 2025

Marco Pedicini — Università Roma Tre

Roma Tre

Laboratory of
Cryptography&Cybersecurity

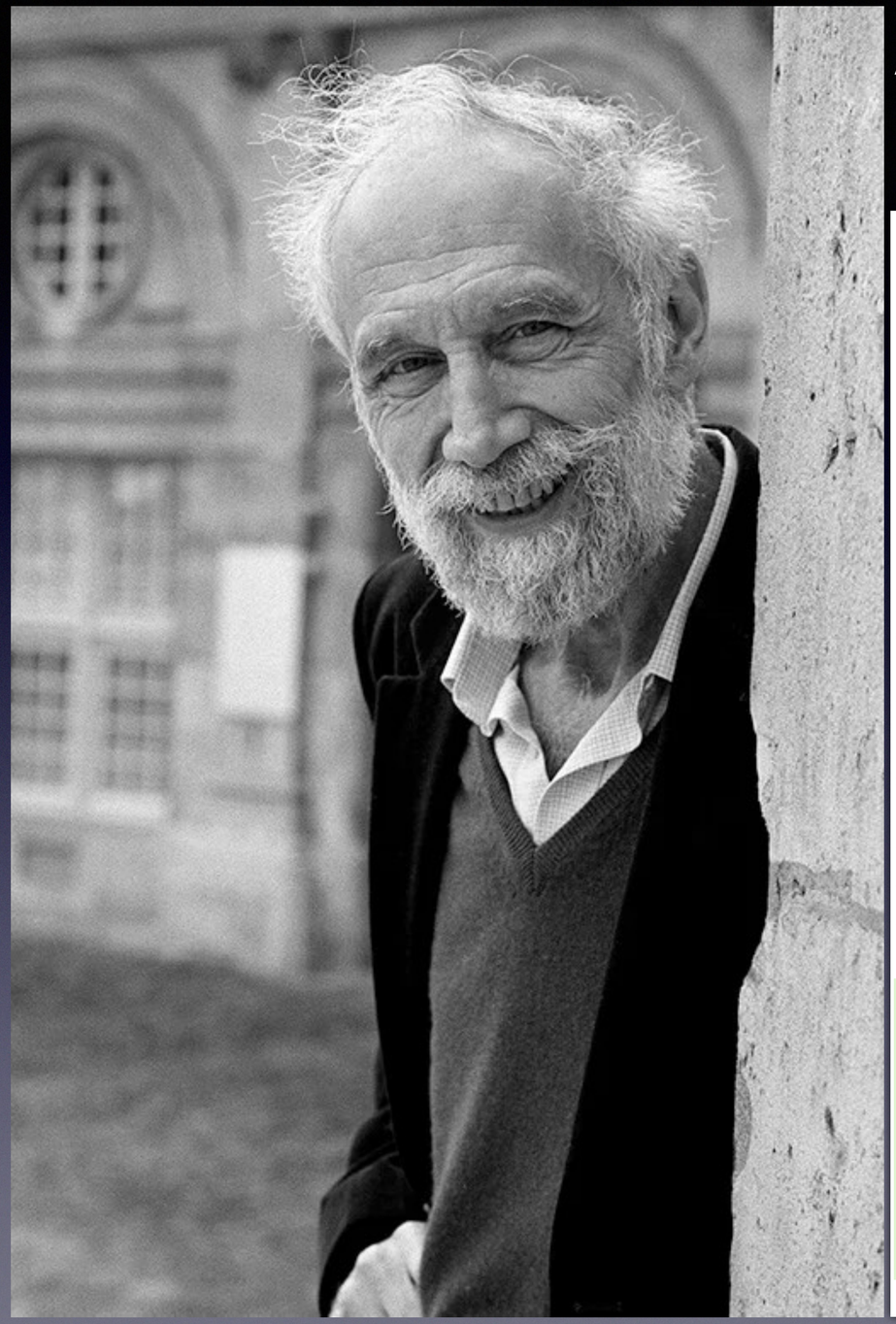
MARCO PEDICINI

DIPARTIMENTO DI
MATEMATICA E FISICA
ROMA TRE UNIVERSITY





https://www.mat.uniroma3.it/users/pedicini/



Alain Connes

Fields Medal 1982

Advice to the beginner

A. Connes

Collège de France, Institut des Hautes Études Scientifiques and Vanderbilt University.

Mathematics is the backbone of modern science and a remarkably efficient source of new concepts and tools to understand the "reality" in which we participate. The new concepts themselves are the result of a long process of "distillation" in the alembic of the human thought.

I was asked to write some advice for young mathematicians. The first observation is that each mathematician is a special case, and in general mathematicians tend to behave like "fermions" *i.e.* avoid working in areas which are too trendy whereas physicists behave a lot more like "bosons" which coalesce in large packs and are often "overselling" their doings, an attitude which mathematicians despise.

It might be tempting at first to view mathematics as the union of separate parts such as Geometry, Algebra, Analysis, Number theory etc... where the first is dominated by the understanding of the concept of "space", the second by the art of manipulating "symbols", the next by the access to "infinity" and the "continuum" etc...

This however does not do justice to one of the most essential features of the mathematical world, namely that it is virtually impossible to isolate any of the above parts from the others without depriving them from their essence. In that way the corpus of mathematics does resemble a biological entity which can only survive as a whole and would perish if separated into disjoint pieces.

The scientific life of mathematicians can be pictured as a trip inside the geography of the "mathematical reality" which they unveil gradually in their own private mental frame.

It often begins by an act of rebellion with respect to the existing dogmatic description of that reality that one will find in existing books. The young "to be mathematician" realize in their own mind that their perception of the mathematical world captures some features which do not quite fit with the existing dogma. This first act is often due in most cases to ignorance but it allows one to free oneself from the reverence to authority by relying on one's intuition provided it is backed up by actual proofs. Once mathematicians get to really know, in an original and "personal" manner, a small part of the mathematical world, as esoteric as it can look at first[1], their trip can really start. It is of course vital all along not to break the "fil d'arianne" which allows to constantly keep a fresh eye on whatever one will encounter along the way, and also to go back to the source if one feels lost at times...

It is also vital to always keep moving. The risk otherwise is to confine oneself in a relatively small area of extreme technical specialization, thus shrinking one's perception of the mathematical world and of its bewildering diversity.

The really *fundamental point* in that respect is that while so many mathematicians have been spending their entire scientific life exploring that world they all agree on its contours and on its connexity: whatever the origin of one's itinerary, one day or another if one walks long enough, one is bound to reach a well known town *i.e.* for instance to meet elliptic functions, modular forms, zeta functions. "All roads lead to Rome" and the mathematical world is "connected". Of course this is not to say that all parts of mathematics look alike and it is worth quoting what Grothendieck says (in "Récoltes et semailles") in comparing the landscape of analysis in which he first worked with that of algebraic geometry in which he spent the rest of his mathematical life:

"Je me rappelle encore de cette impression saisissante (toute subjective certes), comme si je quittais des steppes arides et revêches, pour me retrouver soudain dans une sorte de "pays promis" aux richesses luxuriantes, se multipliant à l'infini partout où il plait à la main de se poser, pour cueillir ou pour fouiller...."

Most mathematicians adopt a pragmatic attitude and see themselves as the explorers of this "mathematical world" whose existence they don't have any wish to question, and whose structure they uncover by a mixture of intuition, not so foreign from "poetical desire"[2], and of a great deal of rationality requiring intense periods of concentration.

Each generation builds a "mental picture" of their own understanding of this world and constructs more and more penetrating mental tools to explore previously hidden aspects of that reality.

Where things get really interesting is when unexpected bridges emerge between parts of the mathematical world that were previously believed to be very far remote from each other in the natural mental picture that a generation had elaborated. At that point one gets the feeling that a sudden wind has blown out the fog that was hiding parts of a beautiful landscape. In my own work this type of "great surprise" came mostly from the interaction with physics. The depth of mathematical concepts that come directly from physics has been qualified in the following terms by Hadamard :

"Not this short lived novelty which can too often influence the mathematician left to his own devices, but this infinitely fecund novelty which springs from the nature of things"

I'll end by some more "practical" advise[3],

- **Walks**

  One very sane exercise, when fighting with a very complicated problem (often involving computations), is to go for a long walk (no paper or pencil) and do the computation in one's head (irrespective of the first feeling "it is too complicated to be done like that"). Even if one does not succeed it trains the "live memory" and sharpens the skills.

- **Lying down**

  Mathematicians usually have a hard time explaining to their partner that the times when they work with most intensity is when they are lying down in the dark on a sofa. Unfortunately with email and the invasion of computer screens in all math. institutes this manner to isolate oneself and concentrate tends to become more rare, it is all the more valuable.

- **Being brave**

  There are several phases in the process leading to "find" new math. and while the "checking" phase is scary and involves just rationality and concentration, the "creative" first phase is of a totally different nature. In some sense it requires a kind of protection of one's ignorance since there are always billions of rational reasons not to look at a problem which has been unsuccessfully looked at by generations of mathematicians.

- **Set backs**

  It does often happen in the life of a mathematician and at any stage (often very early on) of their scientific life, that one for instance gets a "preprint" of a competitor and feels disrupted. The only recipe I have there is to "try" (it is not always easy) to convert this feeling of frustration into positive energy for working harder.

- **Grudging Approbation**

  A colleague of mine once said "We[4] work for the grudging approbation of a few friends". It is true that since the research work is of a rather solitary nature we need badly that approbation in a way or another, but quite frankly don't expect much.... In fact there is no way to fool around with the only real judge which is oneself, and caring too much about the opinion of others is a waste of time: so far no theorem has been proved as a result of a vote. As Feynman put it "why do you care what other people think"!

[1] my starting point was localization of roots of polynomials, but I was fortunately invited at a very early age in a conference in Seattle where I found the roots of all my future work on factors.

[2] as emphasised by the French poet Paul Valery.

[3] recalling that each mathematician is a "special case" don't take the advice too literally.

[4] mathematicians

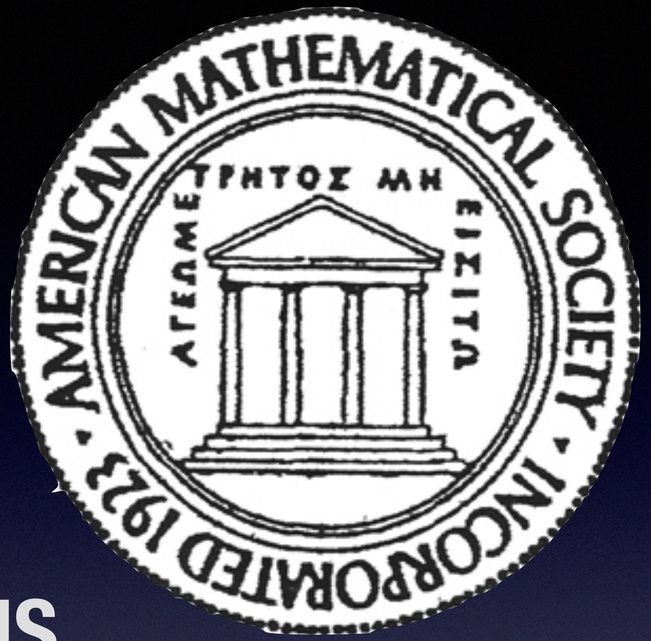
AMS

FREEMAN DYSON IN UN FAMOSO ARTICOLO APPARSO SU **NOTICES OF THE AMS** CLASSIFICA I MATEMATICI IN DUE CATEGORIE:

BIRDS



http://www.ams.org/notices/200902/rtx090200212p.pdf%3Fq%3Dbirds-and-frogs



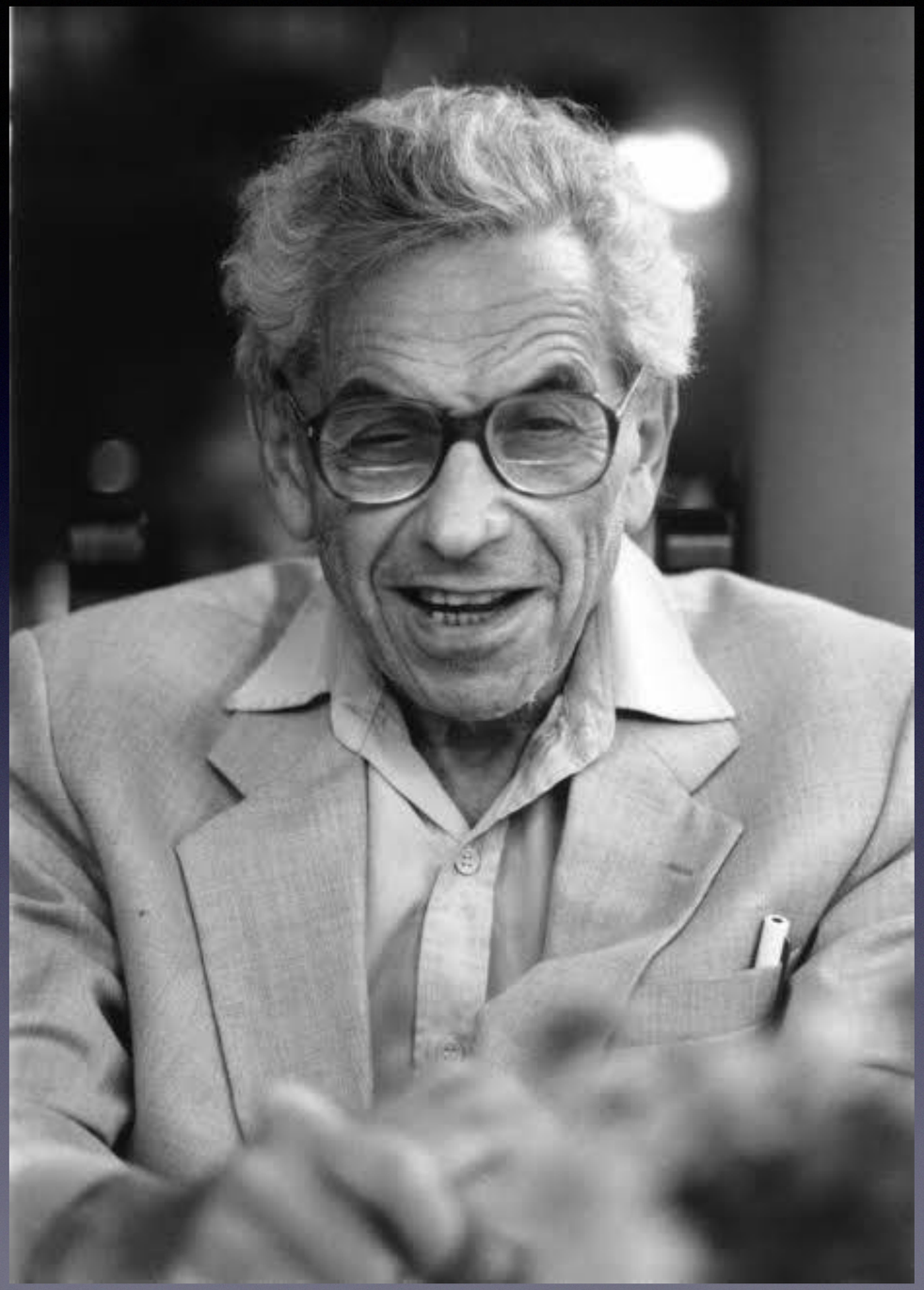
AMS

FREEMAN DYSON IN UN FAMOSO ARTICOLO APPARSO SU NOTICES OF THE AMS CLASSIFICA I MATEMATICI IN DUE CATEGORIE:

FROGS



http://www.ams.org/notices/200902/rtx090200212p.pdf%3Fq%3Dbirds-and-frogs



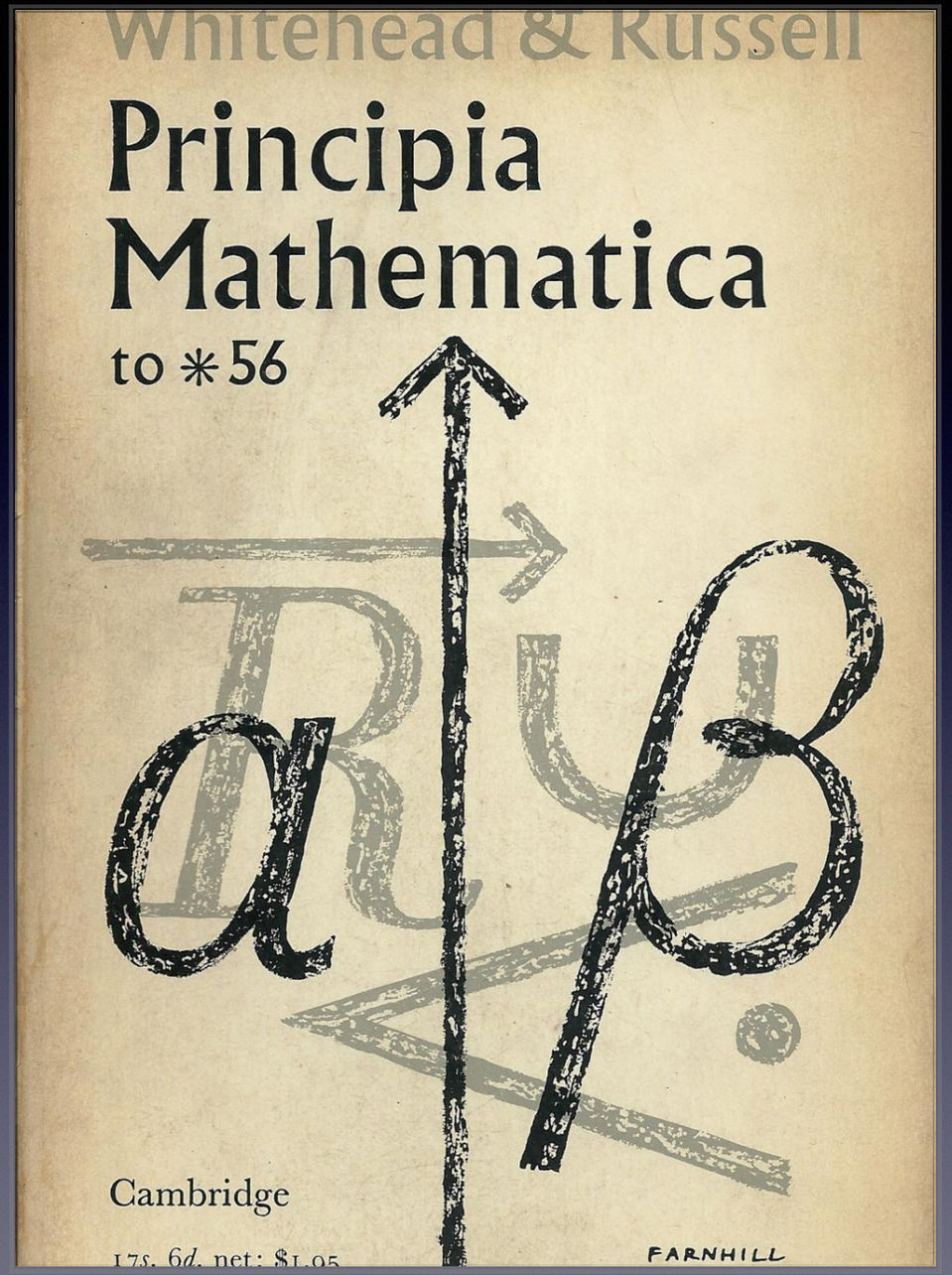
Paul Erdös

https://www.erdosproblems.com/

Di sicuro era “frog”: ha dedicato la sua vita a esplorare una miriade di problemi particolari e specifici (soprattutto nella teoria dei numeri e nella combinatoria), affrontandoli uno a uno con brillante ingegno tecnico piuttosto che con l'architettura di un sistema filosofico-matematico

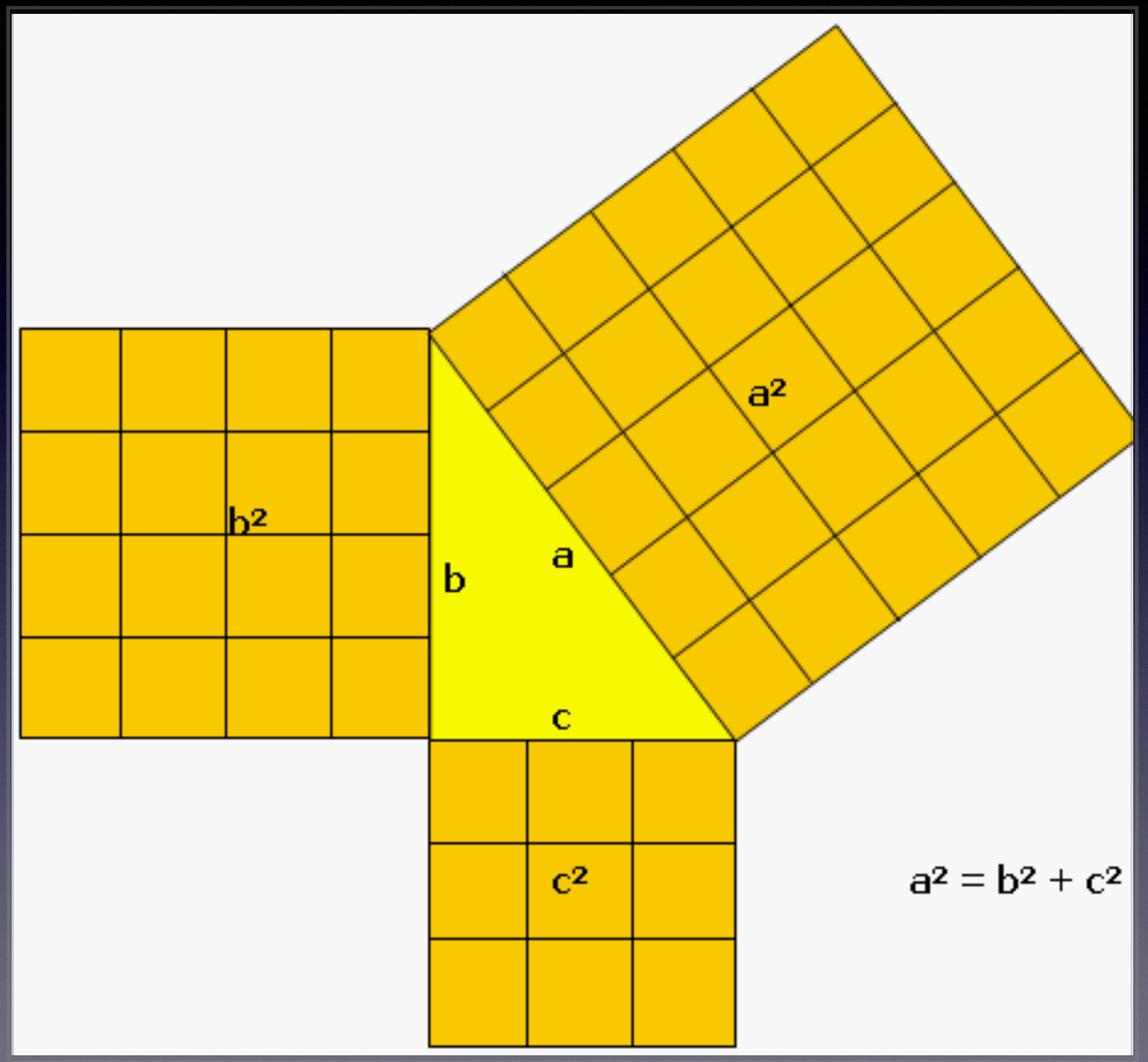
TEOREMI

AFFERMAZIONI DIMOSTRABILI



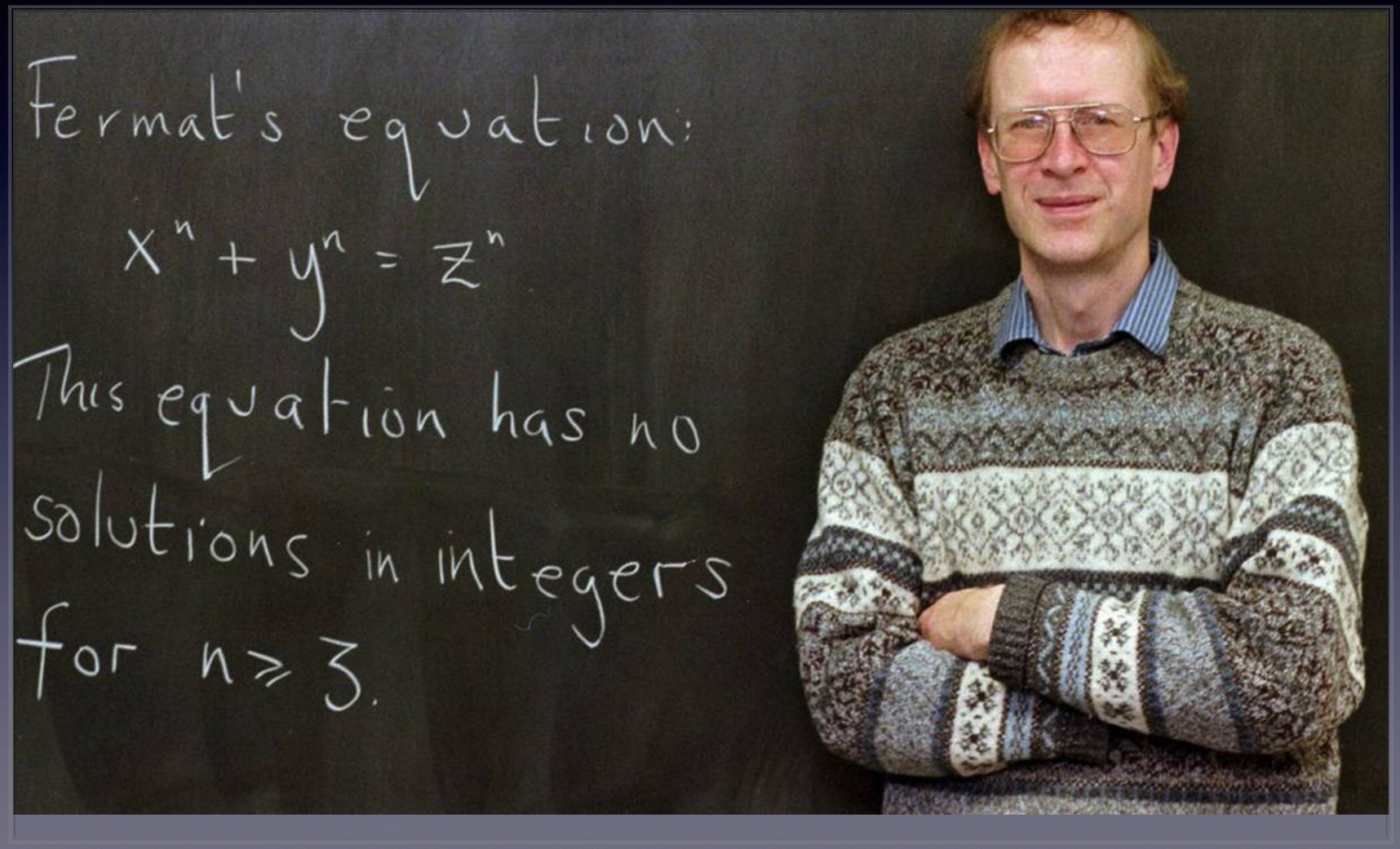
TEOREMI POSITIVI

CI DICONO CHE CERTE PROPRIETÀ SONO VERIFICATE



TEOREMI NEGATIVI

CI DICONO CHE CERTE SITUAZIONI SONO IMPOSSIBILI



Andrew Wiles

insignito di un premio speciale dall'Unione matematica internazionale, la targa d'argento dell'IMU, che gli fu riconosciuto in luogo della prestigiosa medaglia Fields (considerata il massimo riconoscimento per un matematico) in quanto la correzione della dimostrazione fu completata solo nel 1994, anno in cui Wiles aveva più di 40 anni, limite massimo per il conseguimento del premio. Nel 2016 gli fu assegnato il premio Abel "per la sua stupefacente dimostrazione dell'ultimo teorema di Fermat tramite la congettura di modularità per le curve ellittiche semistabili, aprendo una nuova era nella teoria dei numeri"

DIMOSTRAZIONI COME PROGRAMMI
(PROOFS AS PROGRAMS)

COMPUTER SCIENCE

PER I MATEMATICI CHE STUDIANO LA COMPUTER SCIENCE, LE DIMOSTRAZIONI APPAIONO AVERE UNA NATURA DEL TUTTO SIMILE A QUELLA DEI PROGRAMMI.

Structural rules

$$\frac{\Gamma, B, B \vdash \Delta}{\Gamma, B \vdash \Delta}\ cL \qquad \frac{\Gamma \vdash \Delta, B, B}{\Gamma \vdash \Delta, B}\ cR \qquad \frac{\Gamma \vdash \Delta}{\Gamma, B \vdash \Delta}\ wL \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, B}\ wR$$

Identity rules

$$\frac{}{B \vdash B}\ init \qquad \frac{\Gamma \vdash \Delta, B \quad \Gamma, B \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ cut$$

Introduction rules

$$\frac{\Gamma, B_i \vdash \Delta}{\Gamma, B_1 \wedge B_2 \vdash \Delta}\ \wedge L \qquad \frac{\Gamma \vdash \Delta, B \quad \Gamma \vdash \Delta, C}{\Gamma \vdash \Delta, B \wedge C}\ \wedge R \qquad \frac{}{\Gamma \vdash \Delta, t}\ tR$$

$$\frac{\Gamma, B \vdash \Delta \quad \Gamma, C \vdash \Delta}{\Gamma, B \vee C \vdash \Delta}\ \vee L \qquad \frac{}{\Gamma, f \vdash \Delta}\ fL \qquad \frac{\Gamma \vdash \Delta, B_i}{\Gamma \vdash \Delta, B_1 \vee B_2}\ \vee R$$

$$\frac{\Gamma \vdash \Delta, B \quad \Gamma, C \vdash \Delta'}{\Gamma, \Gamma', B \supset C \vdash \Delta, \Delta'}\ \supset L \qquad \frac{\Gamma, B \vdash \Delta, C}{\Gamma \vdash \Delta, B \supset C}\ \supset R$$

$$\frac{\Gamma, [s/x]B \vdash \Delta}{\Gamma, \forall x.B \vdash \Delta}\ \forall L \qquad \frac{\Gamma \vdash \Delta, [y/x]B}{\Gamma \vdash \Delta, \forall x.B}\ \forall R \qquad \frac{\Gamma, [y/x]B \vdash \Delta}{\Gamma, \exists x.B \vdash \Delta}\ \exists L \qquad \frac{\Gamma \vdash \Delta, [s/x]B}{\Gamma \vdash \Delta, \exists x.B}\ \exists R$$

CORRADO BÖHM

NEGLI ANNI ’50, DISEGNÒ UNO DEI PRIMI COMPILATORI BASATO SUL LINGUAGGIO DELLA MATEMATICA.

CORRADO BÖHM

NEGLI ANNI ’50, DISEGNÒ UNO DEI PRIMI COMPILATORI BASATO SUL LINGUAGGIO DELLA MATEMATICA.

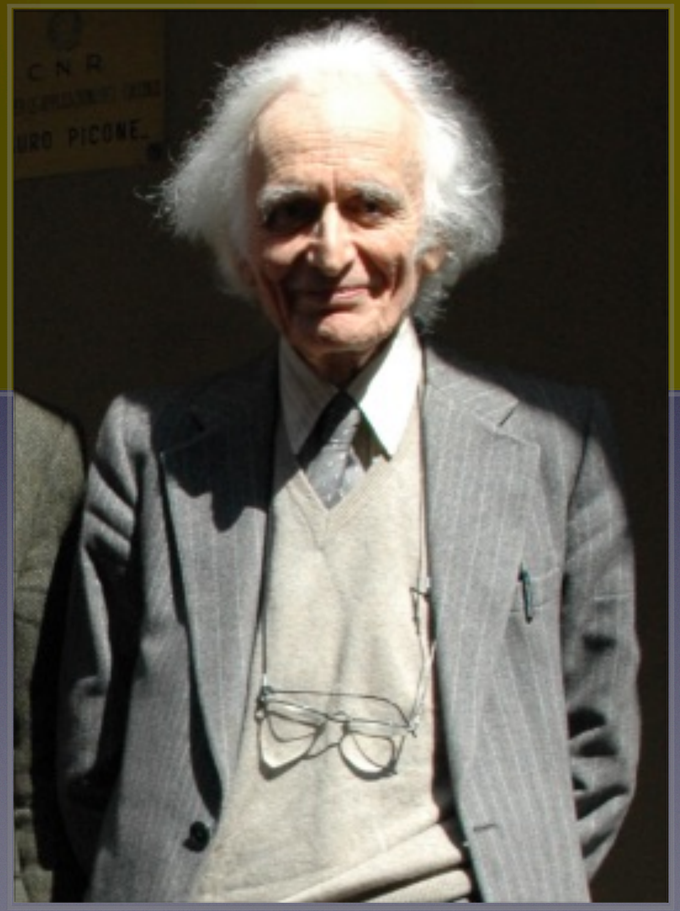
Home > Annali di Matematica Pura ed Applicata > Article

Calculatrices digitales. Du déchiffrage de formules logico-mathématiques par la machine même dans la conception du programme

Published: December 1954

Volume 37, pages 175–217, (1954) Cite this article

Download PDF



CRITTOGRAFIA

UN TEMA SPECIALE CHE COSTITUISCE UN VALIDO ESEMPIO DI SCIENZA COMPUTAZIONALE



CRITTOGRAFIA

UN TEMA SPECIALE CHE COSTITUISCE UN VALIDO ESEMPIO DI SCIENZA COMPUTAZIONALE

LA CRITTOGRAFIA È UN DERIVATO DELLA MATEMATICA, IN MODO SIMILE ALLA COMPUTER SCIENCE, PRODUCE 'ARTIFACTS':



CRITTOGRAFIA

UN TEMA SPECIALE CHE COSTITUISCE UN VALIDO ESEMPIO DI SCIENZA COMPUTAZIONALE

LA CRITTOGRAFIA È UN DERIVATO DELLA MATEMATICA, IN MODO SIMILE ALLA COMPUTER SCIENCE, PRODUCE 'ARTIFACTS':



CRITTOGRAFIA

UN TEMA SPECIALE CHE COSTITUISCE UN VALIDO ESEMPIO DI SCIENZA COMPUTAZIONALE

LA CRITTOGRAFIA È UN DERIVATO DELLA MATEMATICA, IN MODO SIMILE ALLA COMPUTER SCIENCE, PRODUCE 'ARTIFACTS':

SISTEMI DI CIFRATURA



CRITTOGRAFIA

UN TEMA SPECIALE CHE COSTITUISCE UN VALIDO ESEMPIO DI SCIENZA COMPUTAZIONALE

LA CRITTOGRAFIA È UN DERIVATO DELLA MATEMATICA, IN MODO SIMILE ALLA COMPUTER SCIENCE, PRODUCE 'ARTIFACTS':

SISTEMI DI CIFRATURA

LA CRITTOGRAFIA IMPORTA METODI DA VARIE AREE DELLA MATEMATICA (GEOMETRIA, PROBABILITÀ, ALGEBRA, LOGICA).



CRITTOGRAFIA

UN TEMA SPECIALE CHE COSTITUISCE UN VALIDO ESEMPIO DI SCIENZA COMPUTAZIONALE

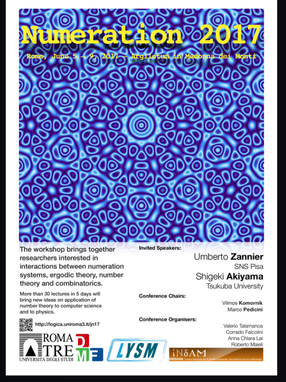
LA CRITTOGRAFIA È UN DERIVATO DELLA MATEMATICA, IN MODO SIMILE ALLA COMPUTER SCIENCE, PRODUCE 'ARTIFACTS':

SISTEMI DI CIFRATURA

LA CRITTOGRAFIA IMPORTA METODI DA VARIE AREE DELLA MATEMATICA (GEOMETRIA, PROBABILITÀ, ALGEBRA, LOGICA).

LA CONOSCENZA E L'UTILIZZO DEI SISTEMI DI CALCOLO (PROGRAMMAZIONE E CALCOLO AD ALTE PRESTAZIONI) SONO AREE INDISPENSABILI.





























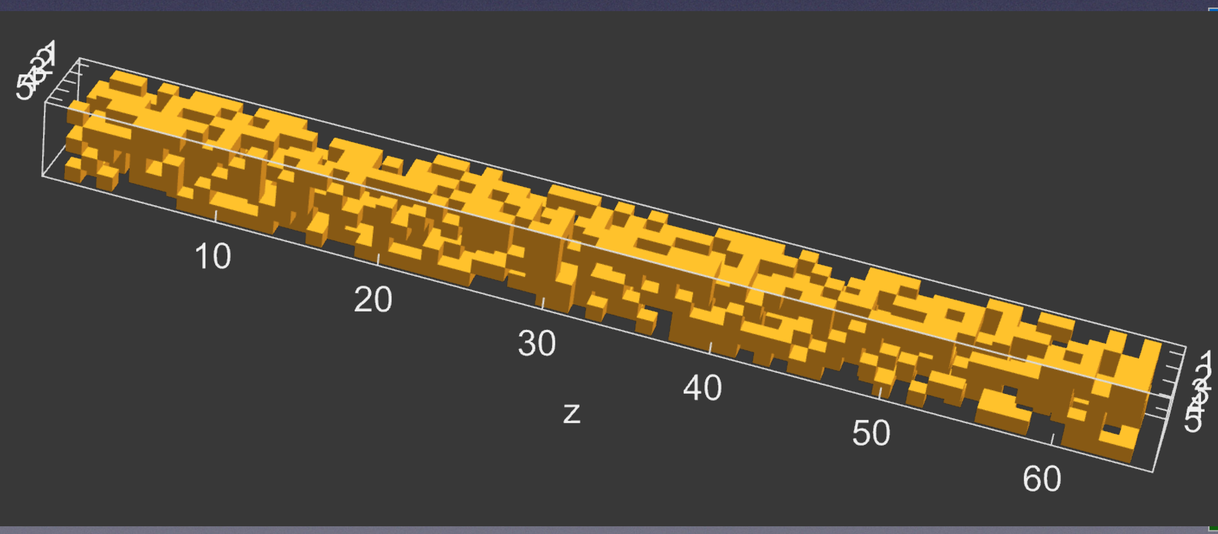












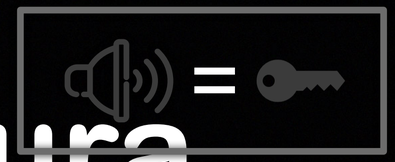
GVCDPMUUZE	KVEMBNVCDZ	CUIJPFLRJA	MNCDEGNDMR	CZTIMYZEZE
YUOVQGYTHV	QZXJACZXVA	MVCIVLHBZA	RLTNREBXOR	AVCQVCURMR
BLGZCCYDXU	CUDIPGZXHR	RATNFCJDIG	SAIVDSLAGN	ZBDINTVVGV
YJWZFYWTQN	GTEDREHGZA	CSAJEBPGXN	ZHAZRLLANH	QJXONPUTHV
APPGFSVVMN	LUTHVAVTIE	GJDDIEPPXP	FLEZEOBTNG	YWPMGCSPNG
MYXVNRATNG	YJDHRPPJNP	GZHZNBHGHN	PLRJARYDLH	CSGZVJKJXN
BPHVIMPPVP	SPUZPCWTMQ	CYEDHBBCVP	GAIVPMTTMV	SZRDFQLPAN

Il nostro obiettivo…

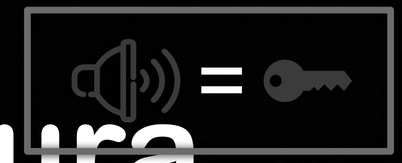
…non è trasformarvi in **crittografi** (almeno per oggi), ma fornirvi una **CASSETTA DEGLI ATTREZZI** di moderne tecniche crittografiche, affinché possiate conoscere alcuni strumenti crittografici che sono disponibili e come si possono applicare.



Il rumore come chiave di cifratura

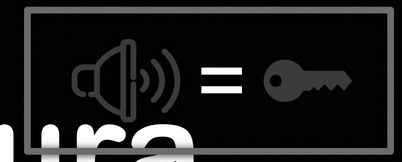


Il rumore come chiave di cifratura





Il rumore come chiave di cifratura



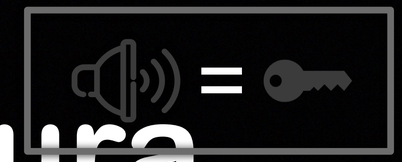


+



Encryption as **adding noise**

Il rumore come chiave di cifratura





Encryption as **adding noise**

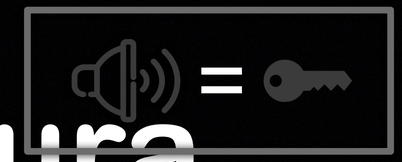
Il rumore come chiave di cifratura



Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**

Il rumore come chiave di cifratura





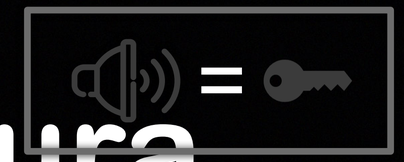
Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**

Sorgente

Destinatario

Il rumore come chiave di cifratura



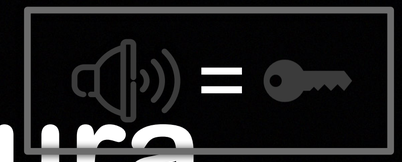


Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**



Il rumore come chiave di cifratura





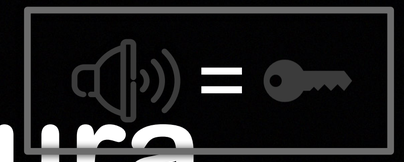
Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**

Sorgente

Destinatario

Il rumore come chiave di cifratura



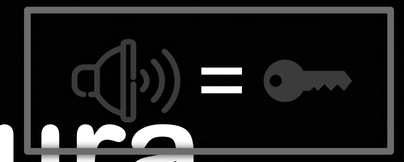


Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**



Il rumore come chiave di cifratura





Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**



Il rumore come chiave di cifratura



Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**



Il rumore come chiave di cifratura



Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**

Il rumore come chiave di cifratura



Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**
- **La sicurezza è misurata in termini di entropia**

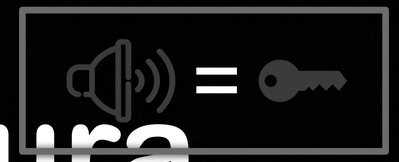
Il rumore come chiave di cifratura



Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**
- **La sicurezza è misurata in termini di entropia**
- **L'entropia è una misura del grado di incertezza.**

Il rumore come chiave di cifratura

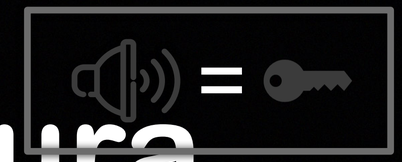




Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**
- **La sicurezza è misurata in termini di entropia**
- **L'entropia è una misura del grado di incertezza.**
- **Quanto più un messaggio è indistinguibile dal rumore, tanto maggiore è la sicurezza.**

Il rumore come chiave di cifratura



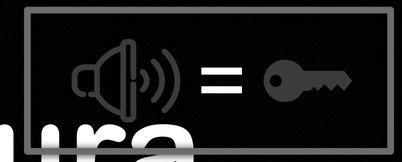


Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**
- **La sicurezza è misurata in termini di entropia**
- **L'entropia è una misura del grado di incertezza.**
- **Quanto più un messaggio è indistinguibile dal rumore, tanto maggiore è la sicurezza.**

- Aggiungere rumore non è necessariamente una perdita di informazioni (se sappiamo tornare indietro).

Il rumore come chiave di cifratura



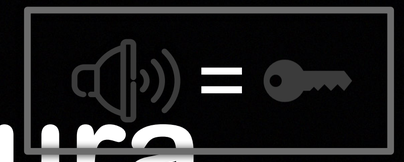


Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**
- **La sicurezza è misurata in termini di entropia**
- **L'entropia è una misura del grado di incertezza.**
- **Quanto più un messaggio è indistinguibile dal rumore, tanto maggiore è la sicurezza.**

- Aggiungere rumore non è necessariamente una perdita di informazioni (se sappiamo tornare indietro).
- È piuttosto una trasformazione che conserva l'entropia fornita dal rumore e la usa per proteggere l’informazione.

Il rumore come chiave di cifratura





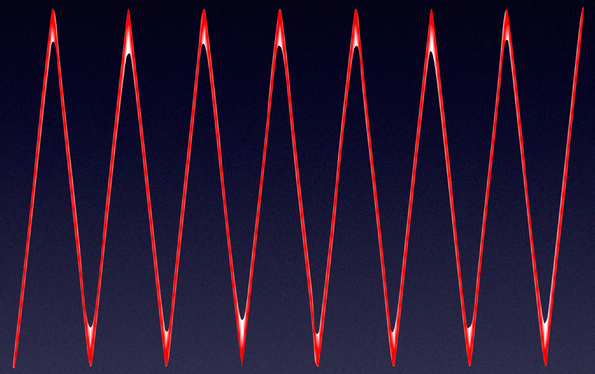
Encryption as **adding noise**

- **Teoria dell'informazione di Claude Shannon**
- **La sicurezza è misurata in termini di entropia**
- **L'entropia è una misura del grado di incertezza.**
- **Quanto più un messaggio è indistinguibile dal rumore, tanto maggiore è la sicurezza.**

- Aggiungere rumore non è necessariamente una perdita di informazioni (se sappiamo tornare indietro).
- È piuttosto una trasformazione che conserva l'entropia fornita dal rumore e la usa per proteggere l’informazione.
- L'informazione è ancora presente, ma inaccessibile senza la chiave (che sarebbe il rumore aggiunto).

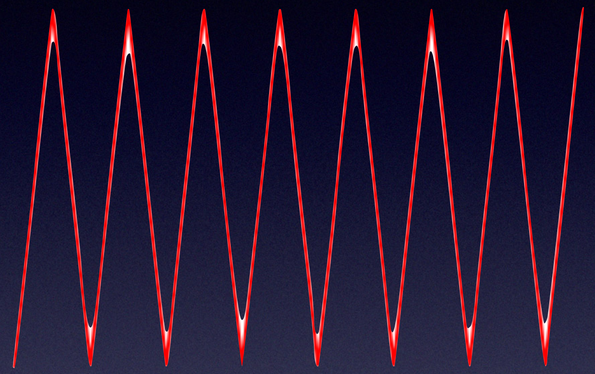
Segnale + rumore (8 bit)

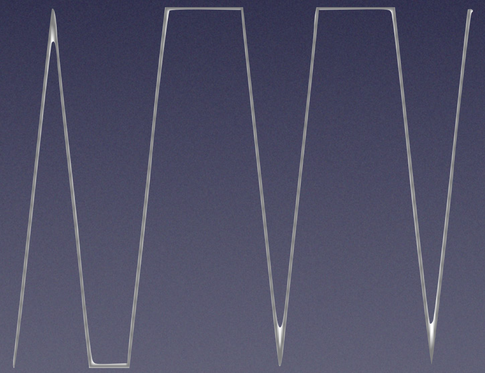
Bassa entropia



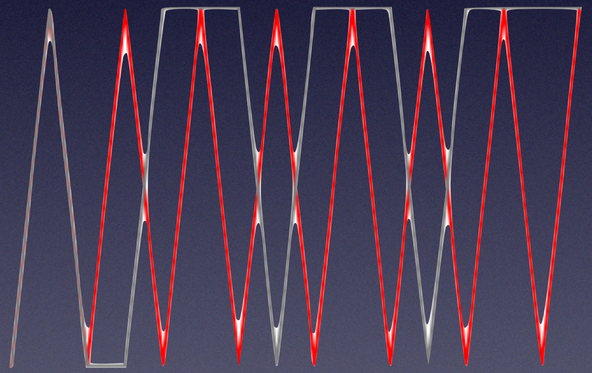
Segnale + rumore (8 bit)

Bassa entropia



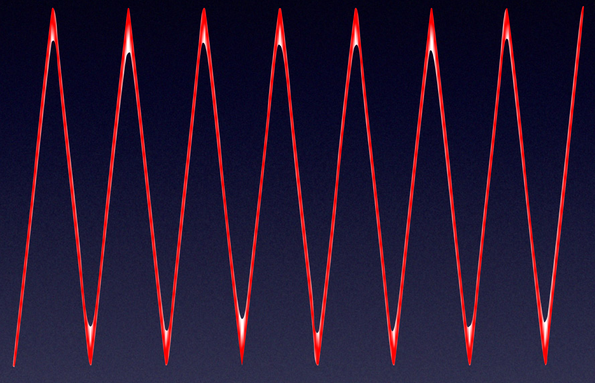


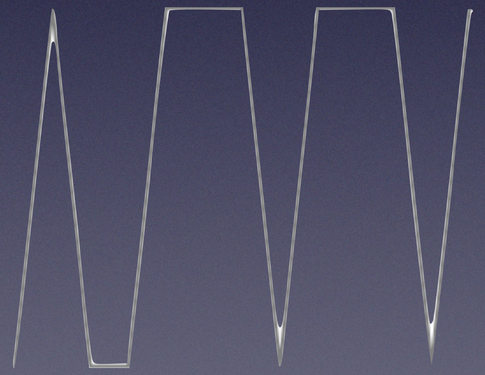
Alta entropia



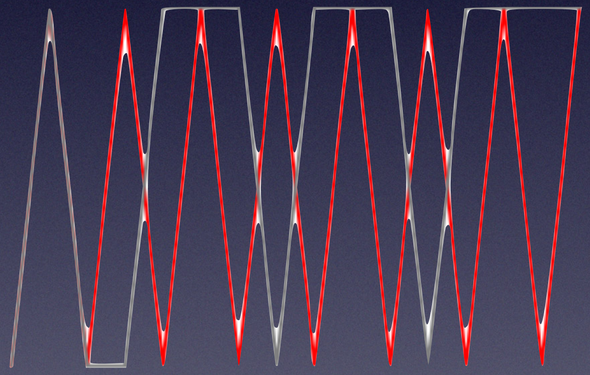
Segnale + rumore (8 bit)

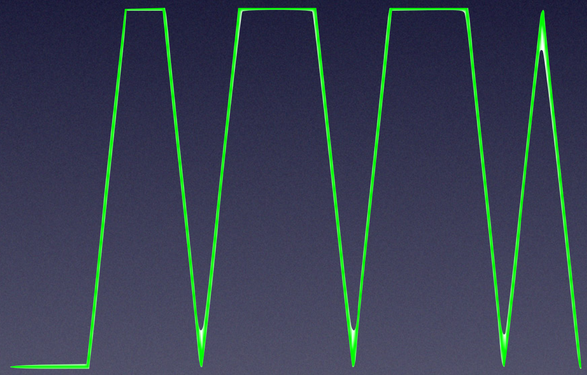
Bassa entropia





Alta entropia

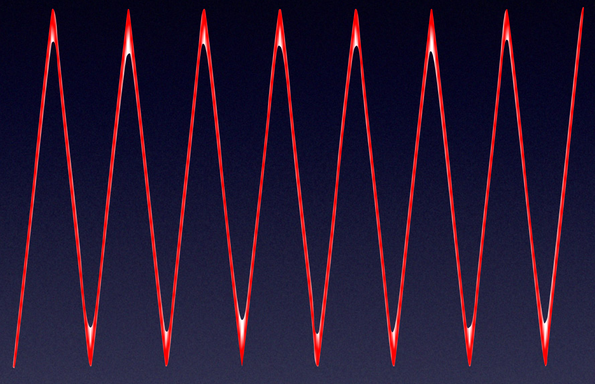




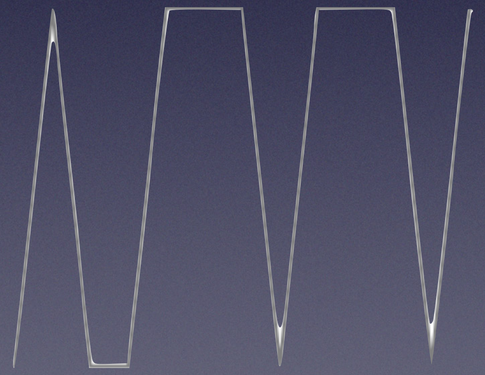
Alta entropia

Segnale + rumore (8 bit)

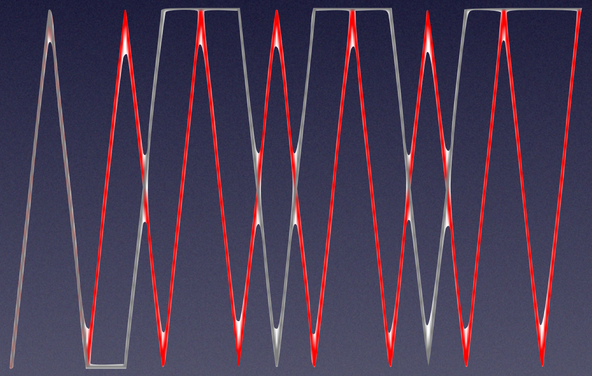
Bassa entropia

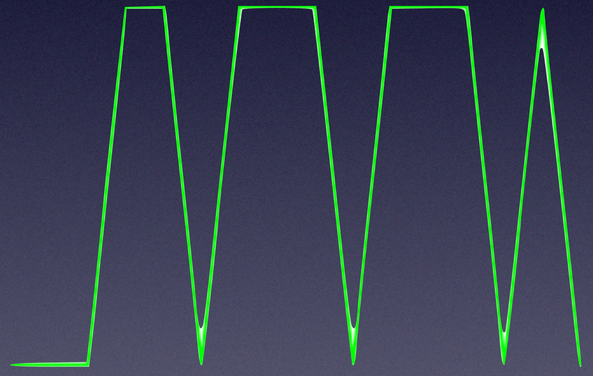


Alta entropia



Segretezza perfetta: il testo cifrato non contiene informazioni sul messaggio

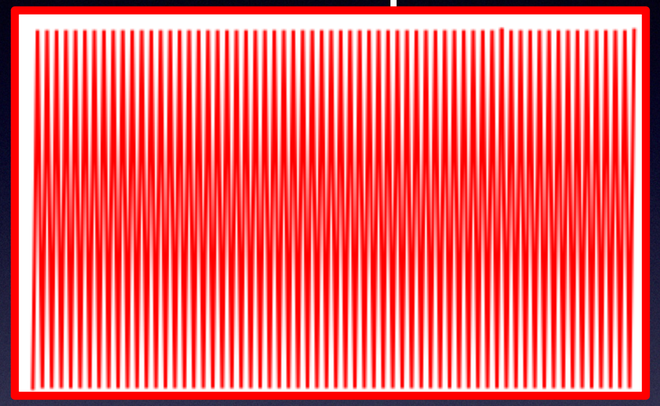




Alta entropia

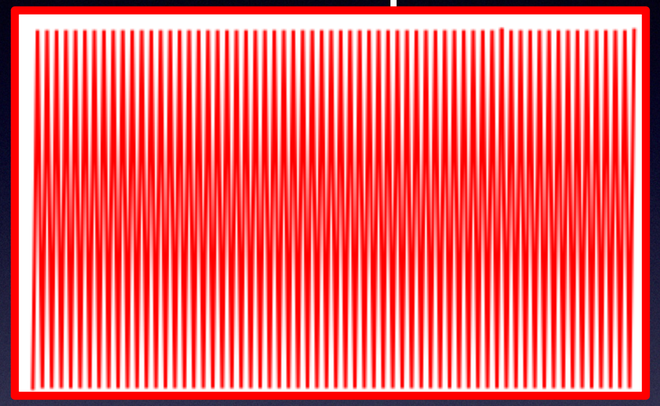
Segnale + rumore (128 bit)

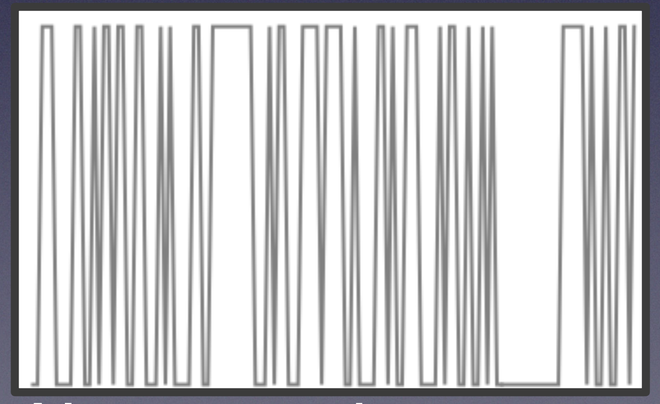
Bassa entropia



Segnale + rumore (128 bit)

Bassa entropia

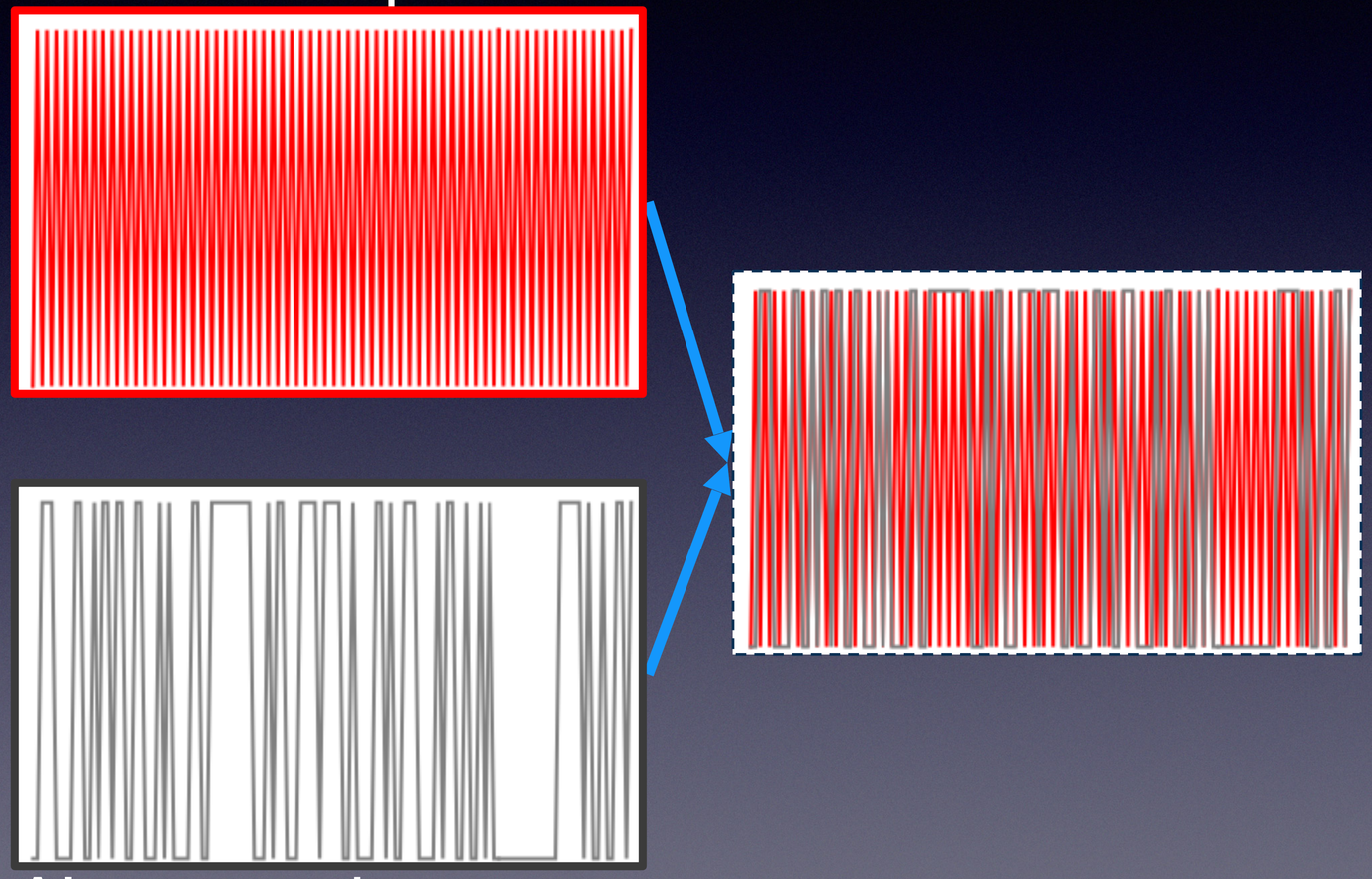




Alta entropia

Segnale + rumore (128 bit)

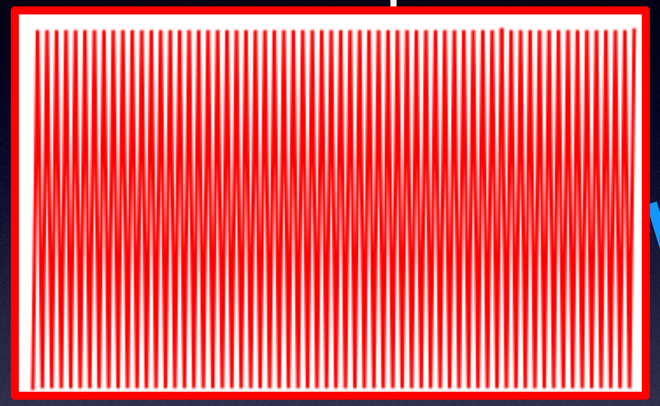
Bassa entropia

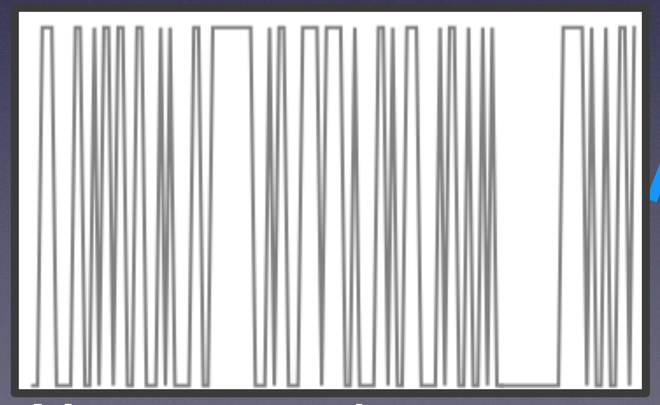


Alta entropia

Segnale + rumore (128 bit)

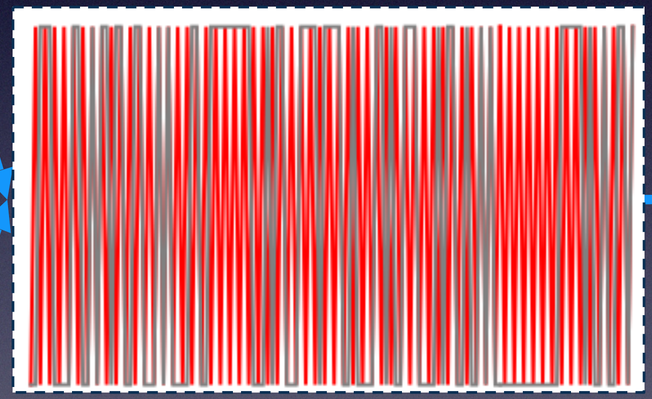
Bassa entropia

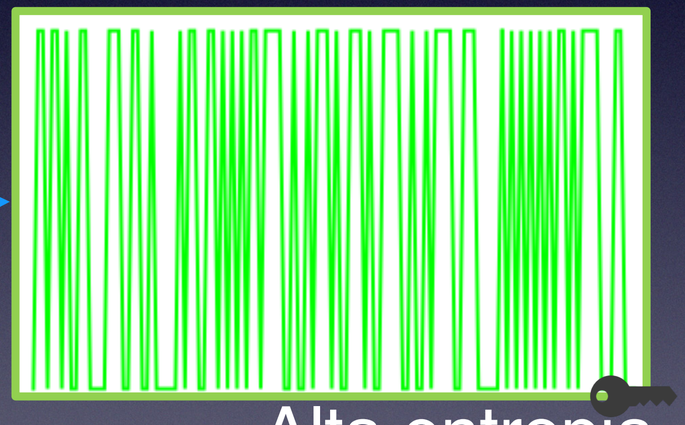




Alta entropia

Segretezza perfetta: il testo cifrato non contiene informazioni sul messaggio

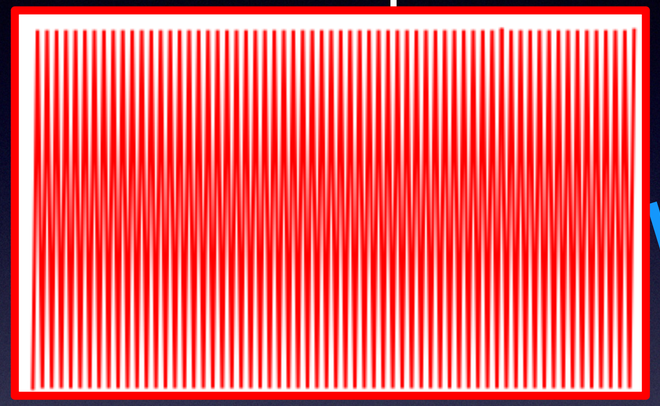


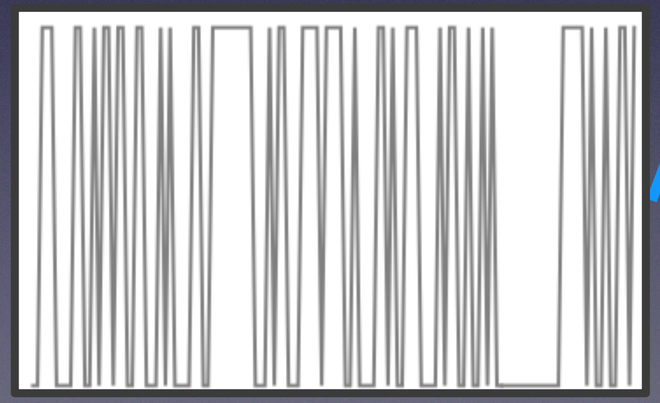


Alta entropia

Segnale + rumore (128 bit)

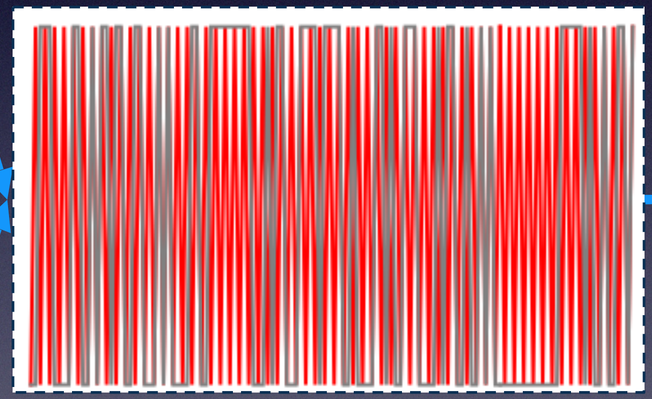
Bassa entropia

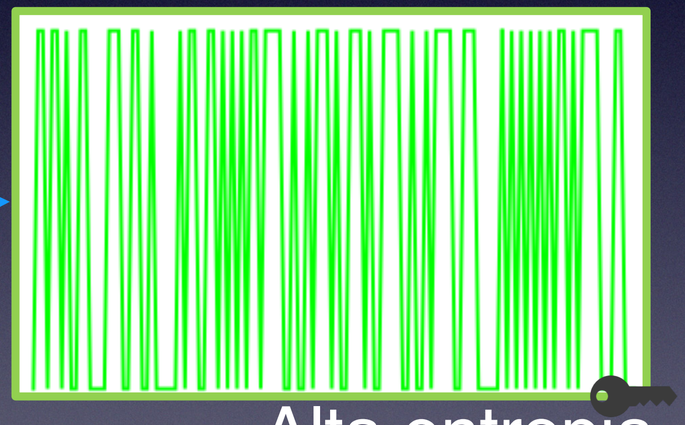




Alta entropia

Segretezza perfetta: il testo cifrato non contiene informazioni sul messaggio



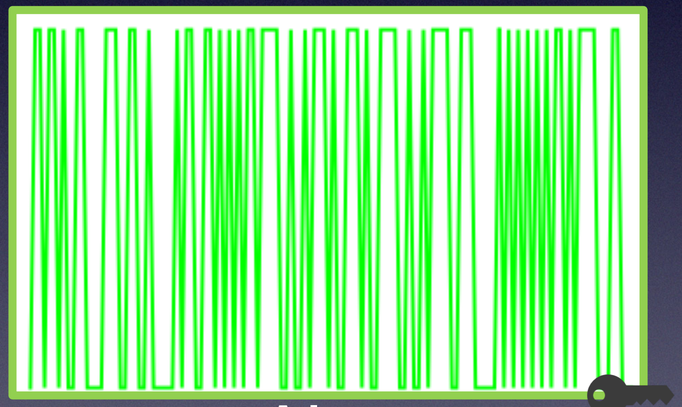


Alta entropia

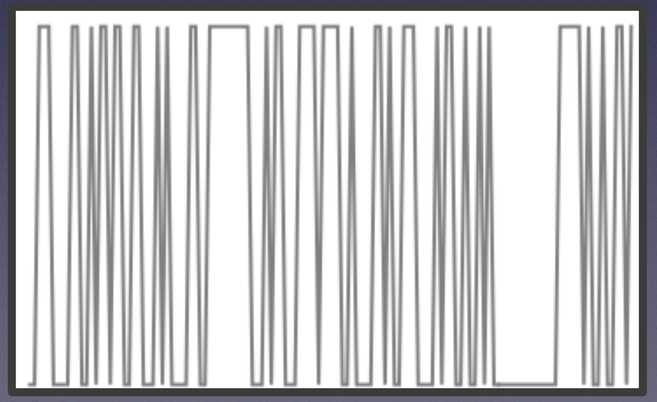
Sicurezza: cifrato come rumore.

Segnale + rumore (128 bit)

Segretezza perfetta: il testo cifrato non contiene informazioni sul messaggio



Alta entropia



Alta entropia

Sicurezza: cifrato come rumore.

Deve essere indistinguibile dal rumore.

Il rumore è un bene?



Il rumore è un bene?

In molti ambiti il rumore è negativo, ma in crittografia ha una connotazione positiva.



Il rumore è un bene?

In molti ambiti il rumore è negativo, ma in crittografia ha una connotazione positiva.
Dobbiamo fare attenzione:



Il rumore è un bene?

In molti ambiti il rumore è negativo, ma in crittografia ha una connotazione positiva.
Dobbiamo fare attenzione:



Il rumore è un bene?



In molti ambiti il rumore è negativo, ma in crittografia ha una connotazione positiva.
Dobbiamo fare attenzione:

il modo in cui viene aggiunto il rumore è importante.

Il rumore è un bene?



In molti ambiti il rumore è negativo, ma in crittografia ha una connotazione positiva.
Dobbiamo fare attenzione:

il modo in cui viene aggiunto il rumore è importante.

Il rumore è un bene?



In molti ambiti il rumore è negativo, ma in crittografia ha una connotazione positiva.
Dobbiamo fare attenzione:

il modo in cui viene aggiunto il rumore è importante.

A seconda delle operazioni sul rumore:

Il rumore è un bene?



In molti ambiti il rumore è negativo, ma in crittografia ha una connotazione positiva.
Dobbiamo fare attenzione:

il modo in cui viene aggiunto il rumore è importante.

A seconda delle operazioni sul rumore:
RUMORE + RUMORE è ancora RUMORE

Il rumore è un bene?



In molti ambiti il rumore è negativo, ma in crittografia ha una connotazione positiva.
Dobbiamo fare attenzione:

il modo in cui viene aggiunto il rumore è importante.

A seconda delle operazioni sul rumore:
RUMORE + RUMORE è ancora RUMORE
aggiungere rumore non riduce l'entropia finale

Il rumore è un bene?

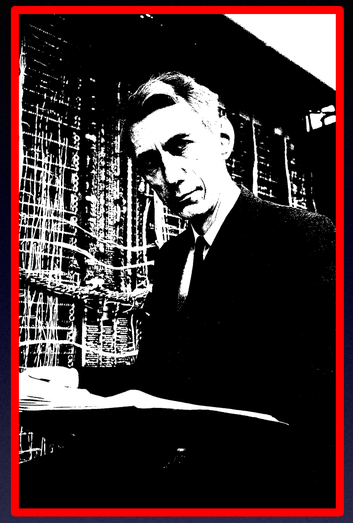


In molti ambiti il rumore è negativo, ma in crittografia ha una connotazione positiva.
Dobbiamo fare attenzione:

il modo in cui viene aggiunto il rumore è importante.

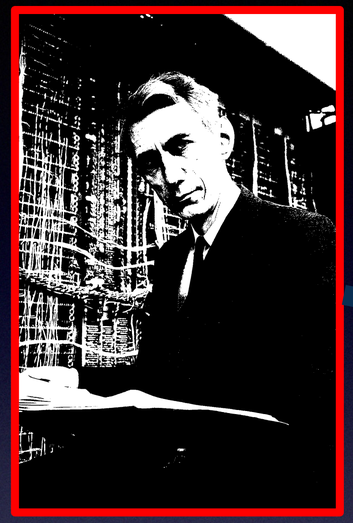
A seconda delle operazioni sul rumore:
RUMORE + RUMORE è ancora RUMORE
aggiungere rumore non riduce l'entropia finale
aggiungere troppo rumore può rendere impossibile la decifratura.

Segnale + rumore

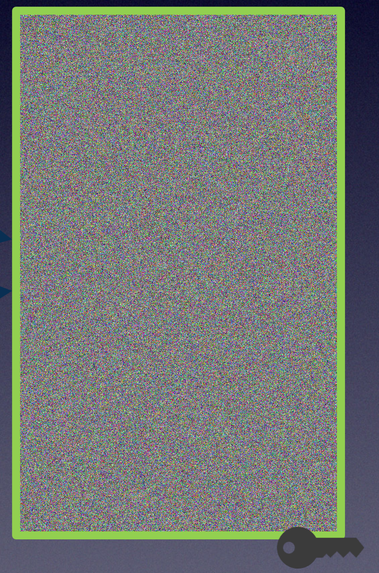




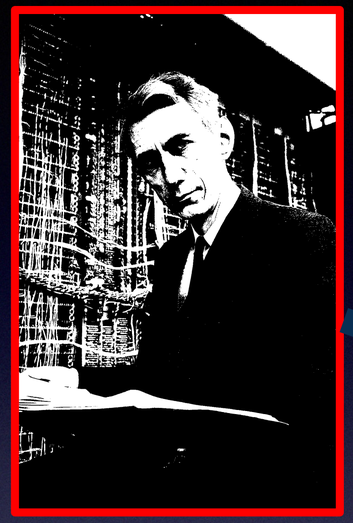
Segnale + rumore



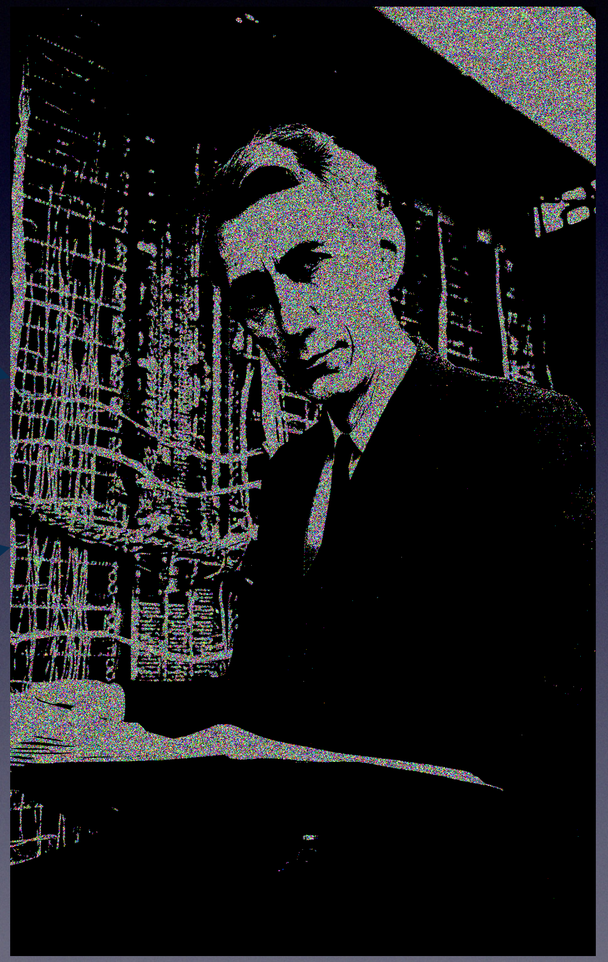




Segnale + rumore

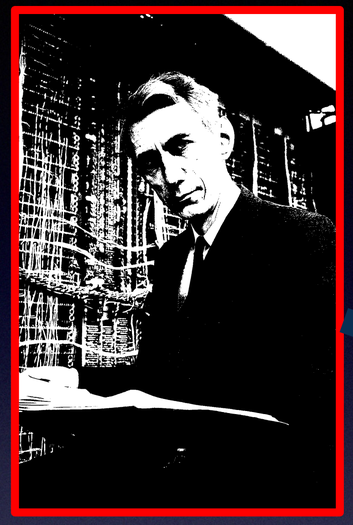




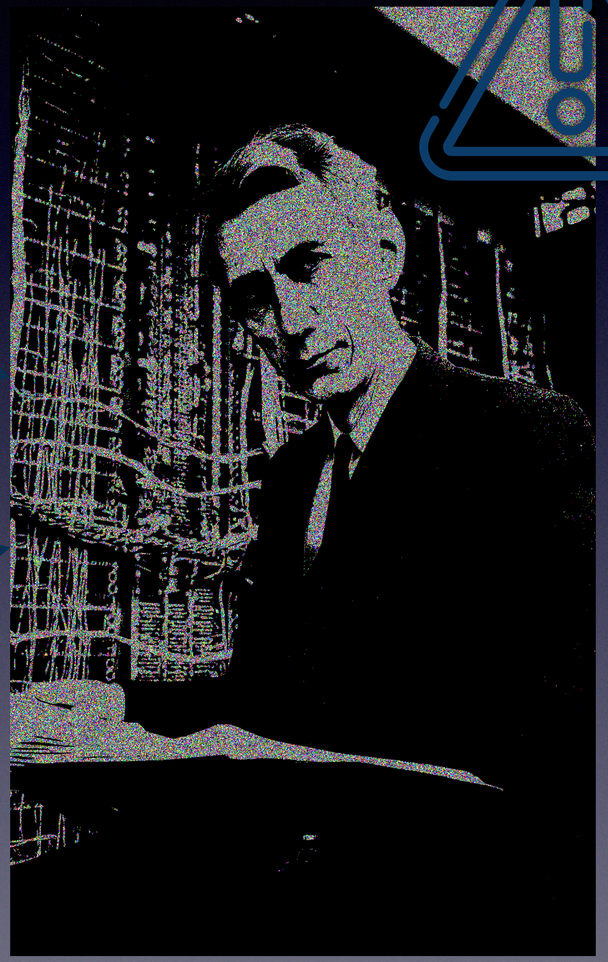


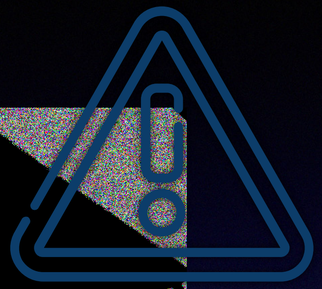


Segnale + rumore





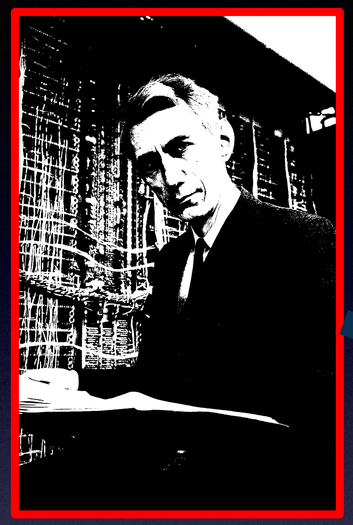




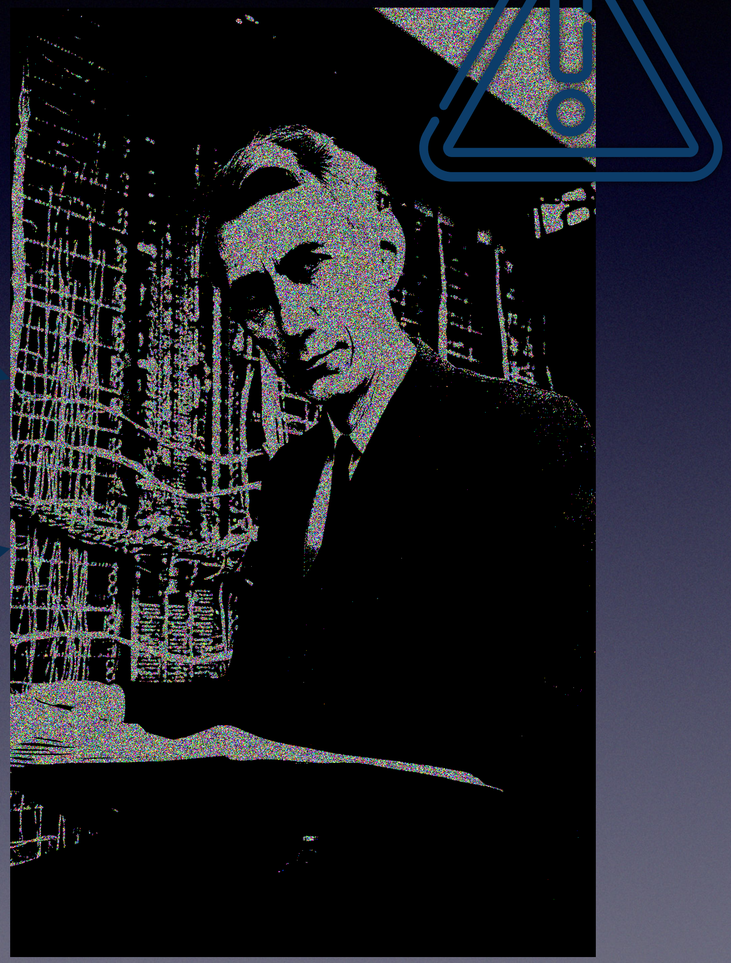


AND logico bit a bit

Segnale + rumore







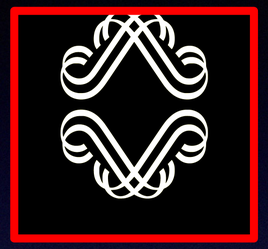


AND logico bit a bit

XOR logico bit a bit

Uno «schema proto-omomorfico»

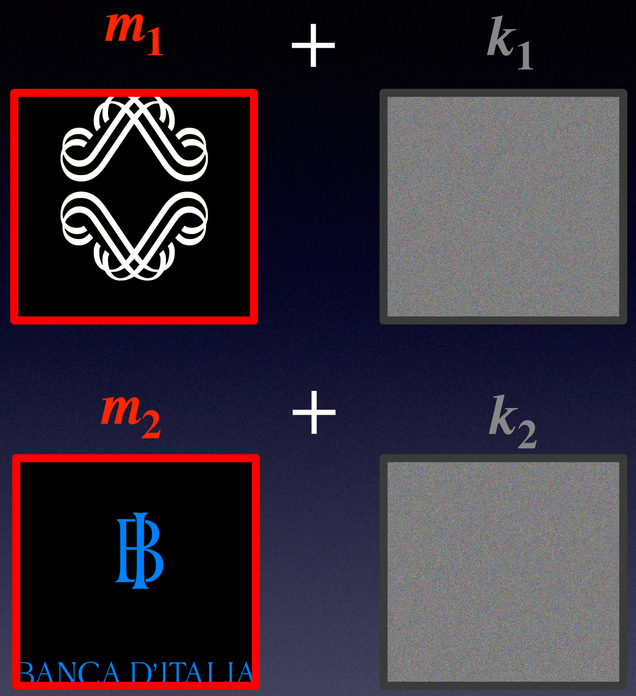
m_1



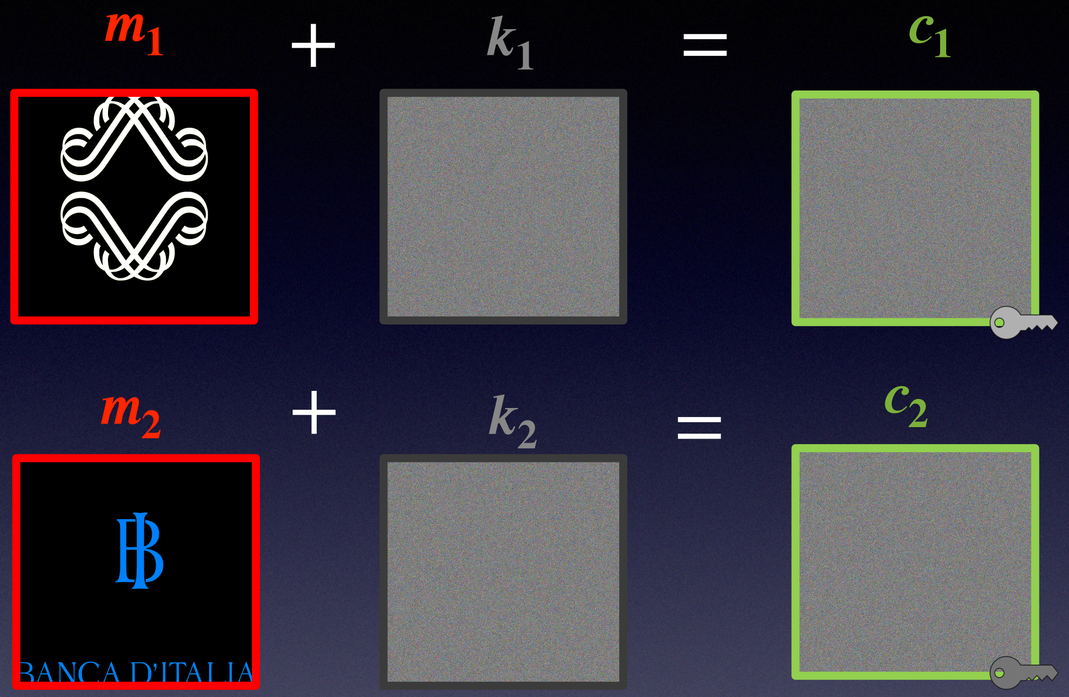
m_2



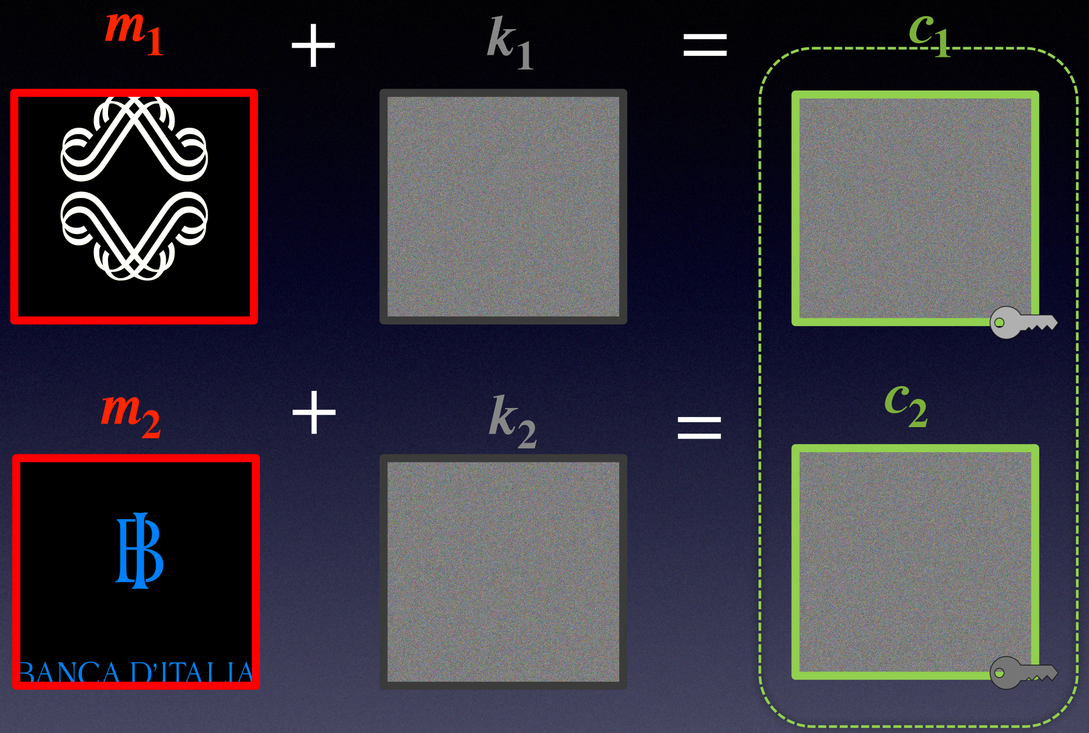
Uno «schema proto-omomorfico»

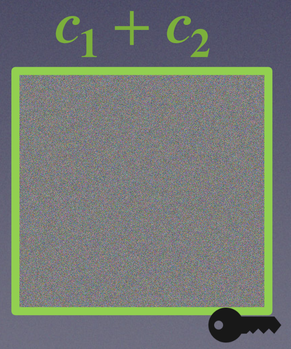


Uno «schema proto-omomorfico»

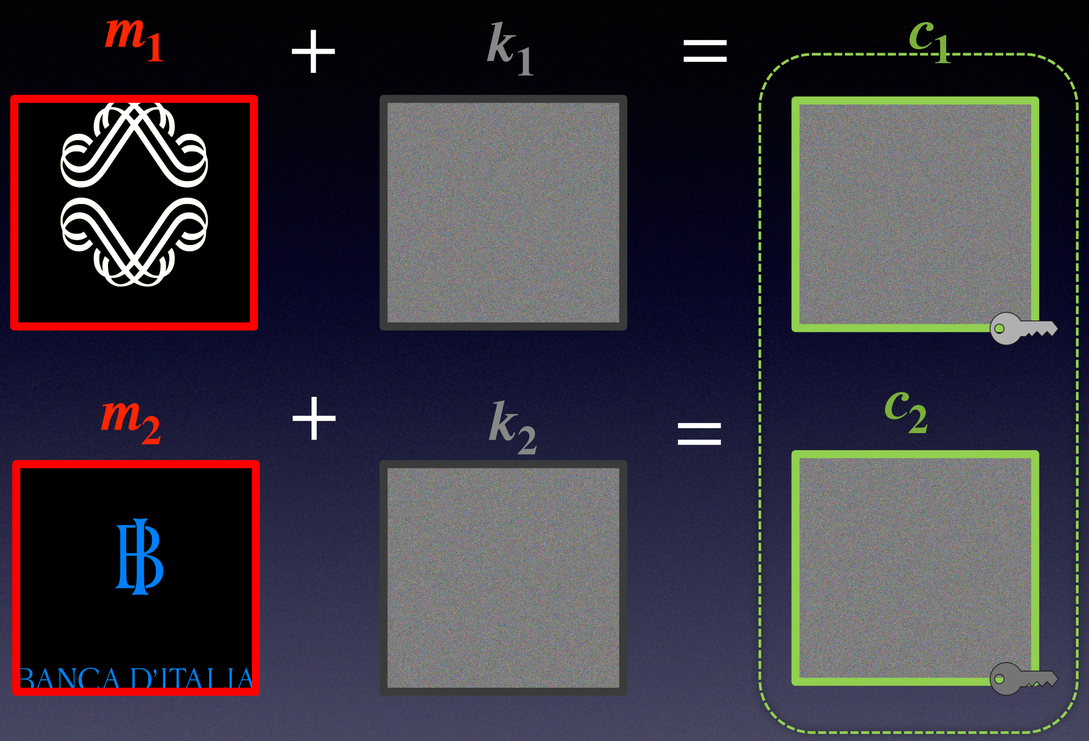


Uno «schema proto-omomorfico»





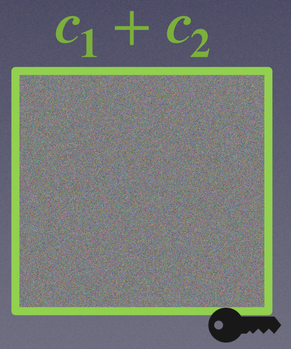
Uno «schema proto-omomorfico»



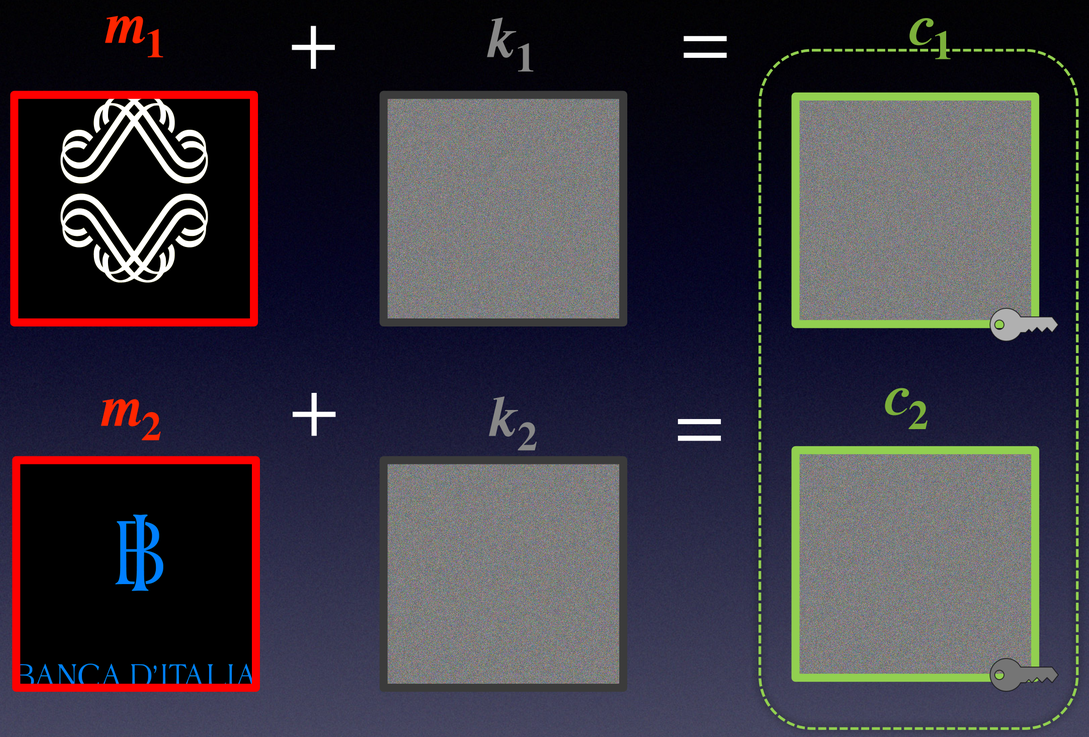
LA MALLEABILITÀ NON È UNA VULNERABILITÀ:

È UNA FUNZIONALITÀ.



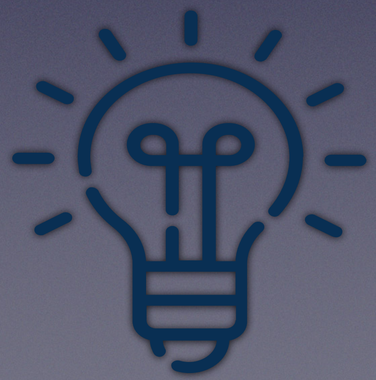


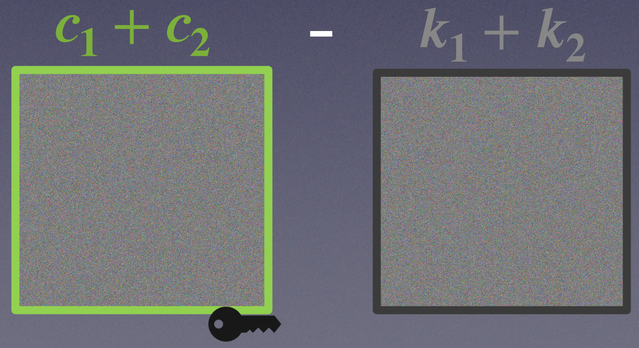
Uno «schema proto-omomorfico»



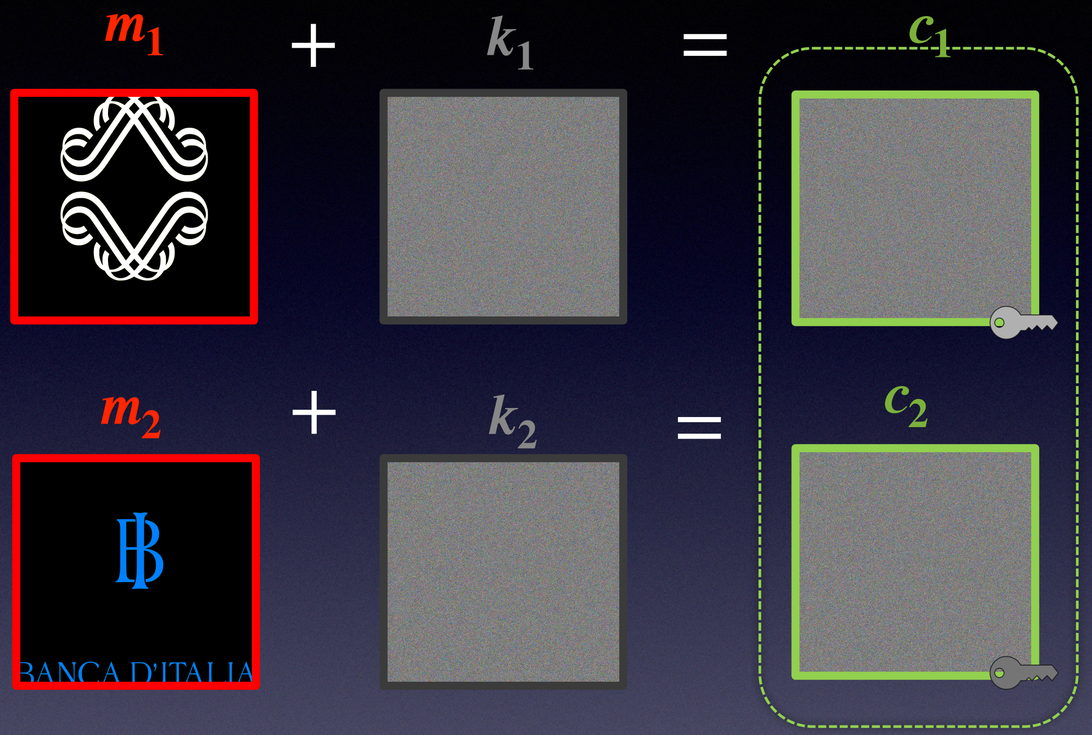
LA MALLEABILITÀ NON È UNA VULNERABILITÀ:

È UNA FUNZIONALITÀ.





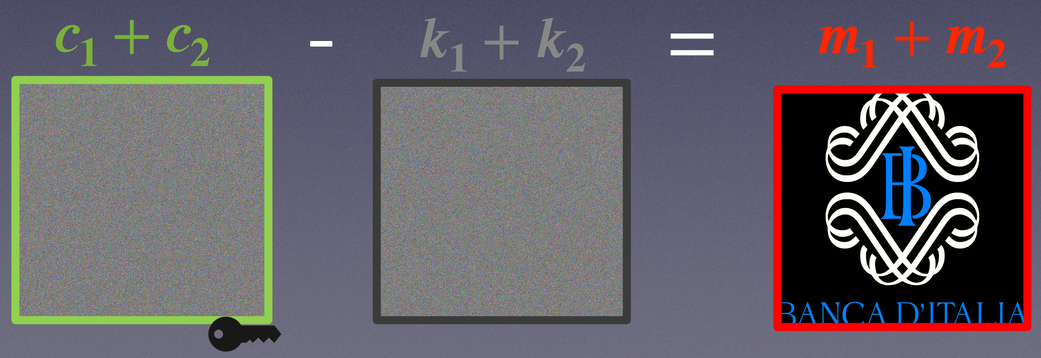
Uno «schema proto-omomorfico»



LA MALLEABILITÀ NON È UNA VULNERABILITÀ:

È UNA FUNZIONALITÀ.



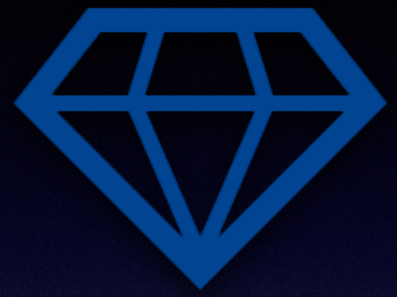


Domanda

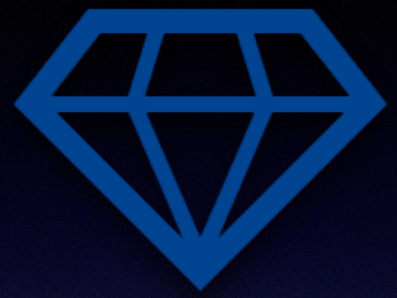
Possiamo ottenere questa proprietà per ogni funzione di combinazione?

«Cifrato per sempre»

«Cifrato per sempre»

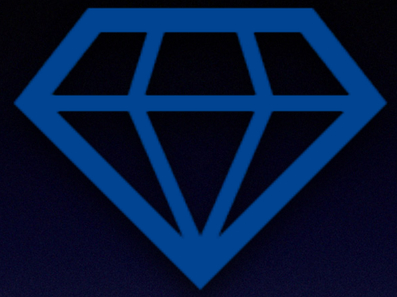


«Cifrato per sempre»



FHE

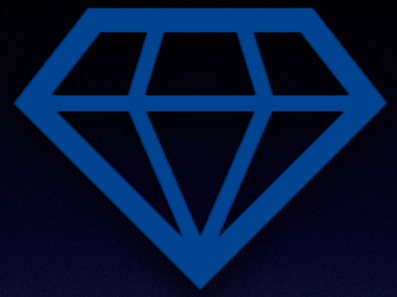
«Cifrato per sempre»



FHE

ZKP

«Cifrato per sempre»

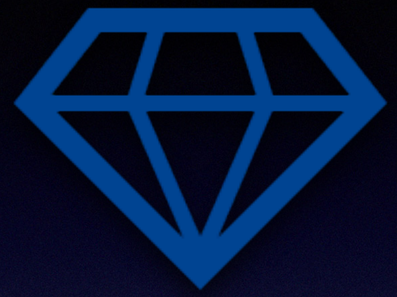


FHE

ZKP

DP

«Cifrato per sempre»



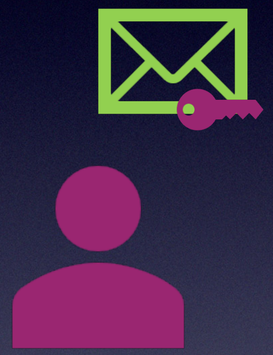
FHE

ZKP

SMPC

DP

Non è ancora la nostra realtà

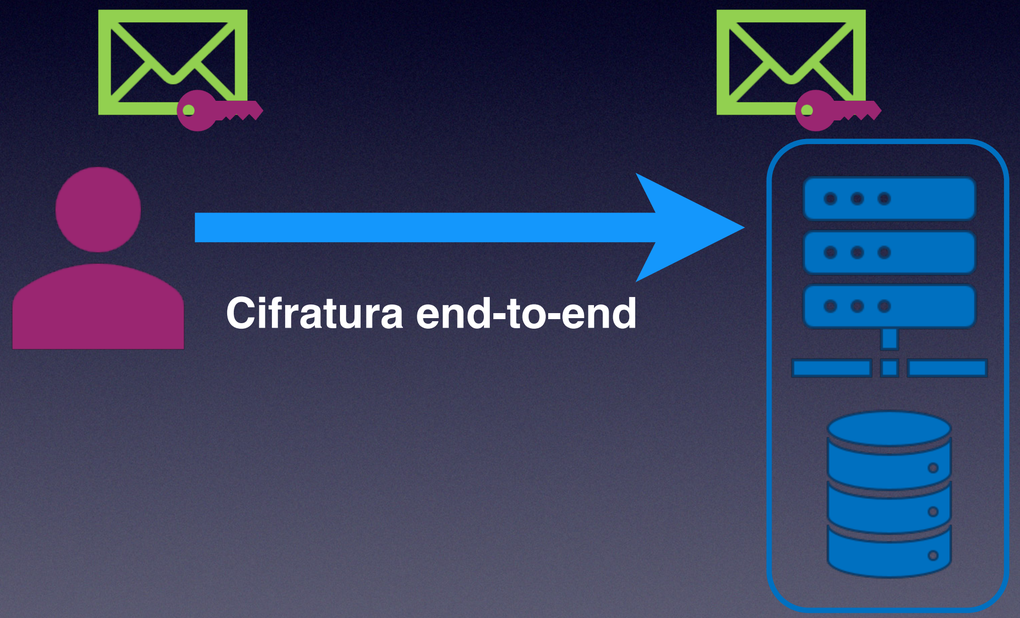




Quando i dati tornano in chiaro, sono vulnerabili.

Rischi e sfide normative

Non è ancora la nostra realtà

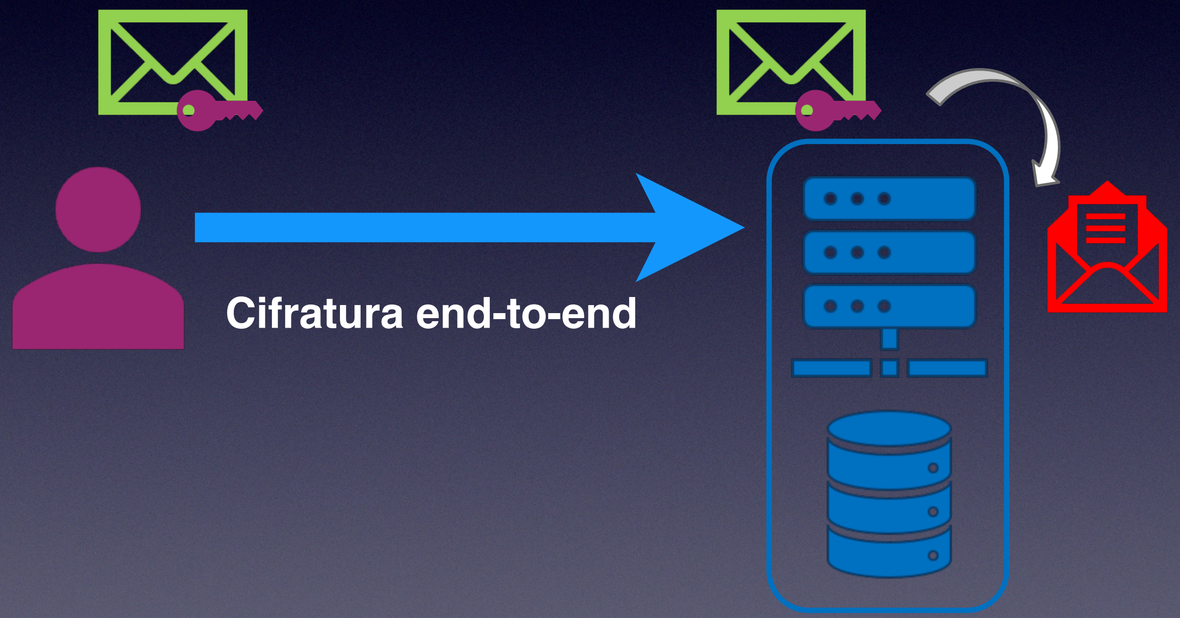




Quando i dati tornano in chiaro, sono vulnerabili.

Rischi e sfide normative

Non è ancora la nostra realtà

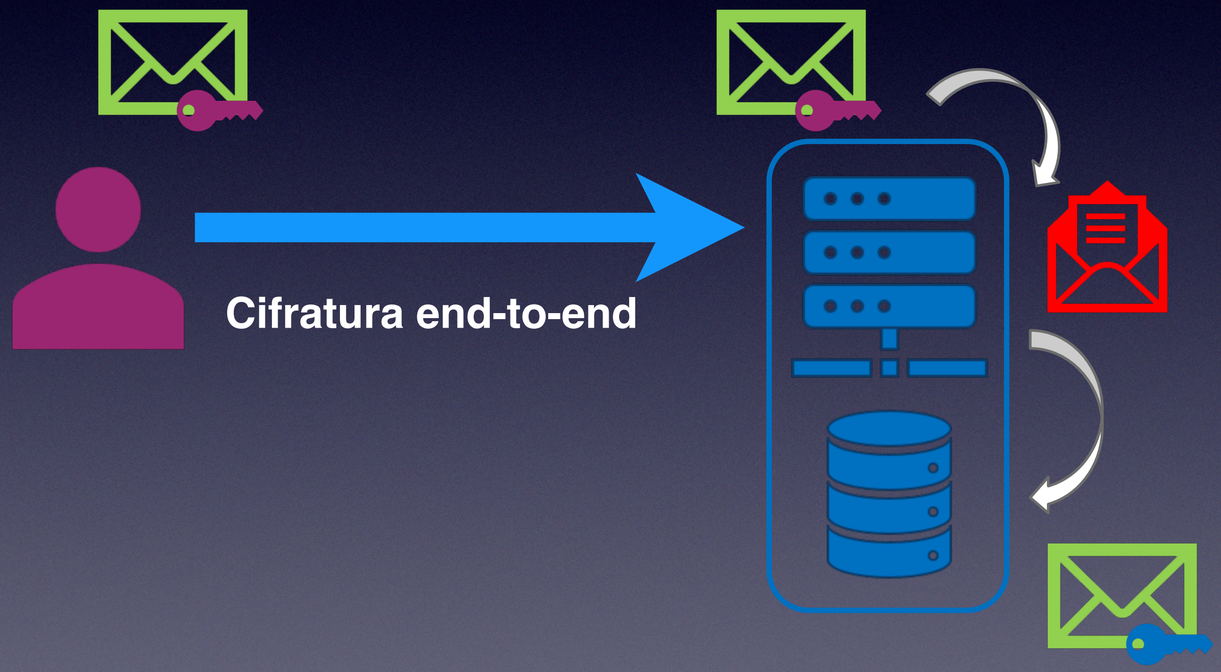




Quando i dati tornano in chiaro, sono vulnerabili.

Rischi e sfide normative

Non è ancora la nostra realtà





Quando i dati tornano in chiaro, sono vulnerabili.

Rischi e sfide normative

Non è ancora la nostra realtà



Utah NSA Data Center

Non è ancora la nostra realtà

Gli avversari intercettano e conservano grandi quantità di dati cifrati, senza preoccuparsi di non poterli leggere immediatamente.



Utah NSA Data Center

Non è ancora la nostra realtà

Gli avversari intercettano e conservano grandi quantità di dati cifrati, senza preoccuparsi di non poterli leggere immediatamente.



Utah NSA Data Center

Non è ancora la nostra realtà

Gli avversari intercettano e conservano grandi quantità di dati cifrati, senza preoccuparsi di non poterli leggere immediatamente.

Con l'aumento della potenza di calcolo, ciò che oggi è indecifrabile potrebbe diventare leggibile domani.



Utah NSA Data Center

Non è ancora la nostra realtà

Gli avversari intercettano e conservano grandi quantità di dati cifrati, senza preoccuparsi di non poterli leggere immediatamente.

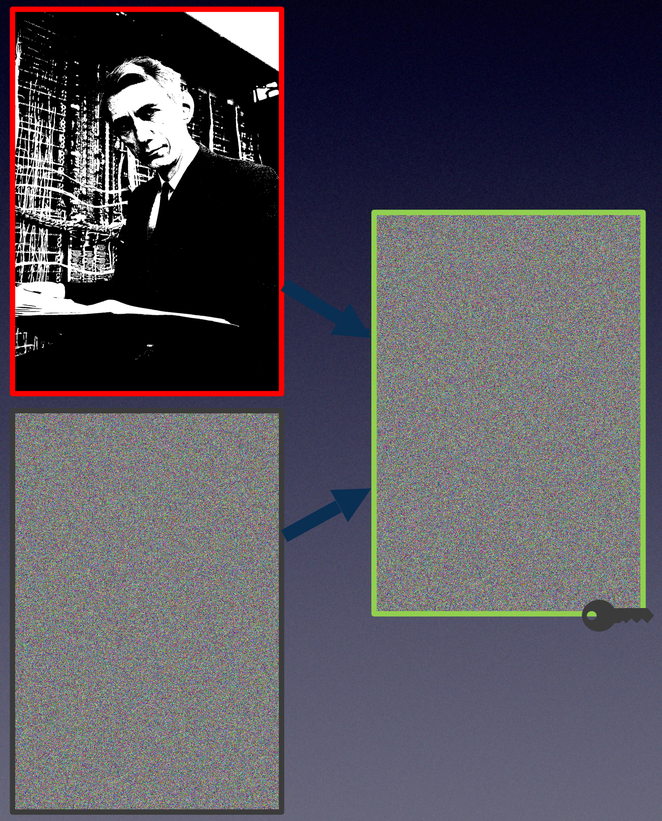
Con l'aumento della potenza di calcolo, ciò che oggi è indecifrabile potrebbe diventare leggibile domani.



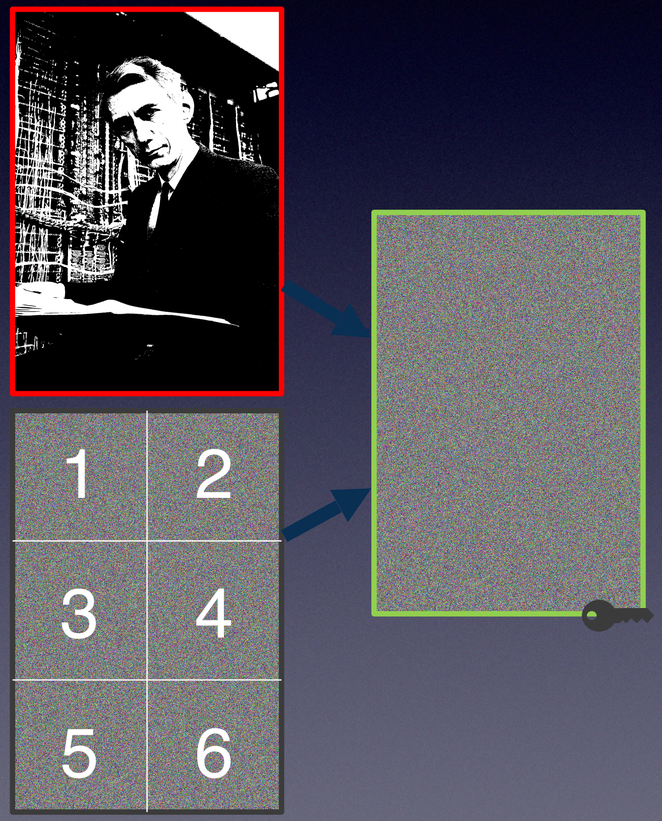
Utah NSA Data Center

RACCOGLI ORA, DECIFRA DOPO

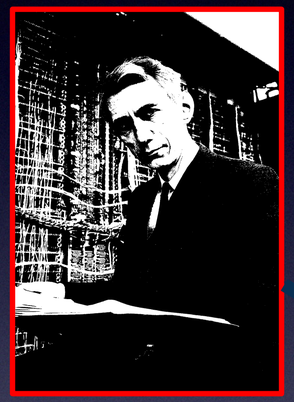
Rumore distribuito (condivisione del segreto)



Rumore distribuito (condivisione del segreto)

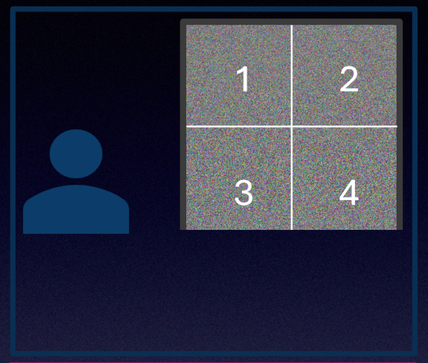


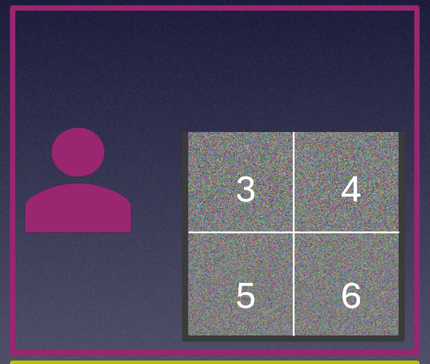
Rumore distribuito (condivisione del segreto)

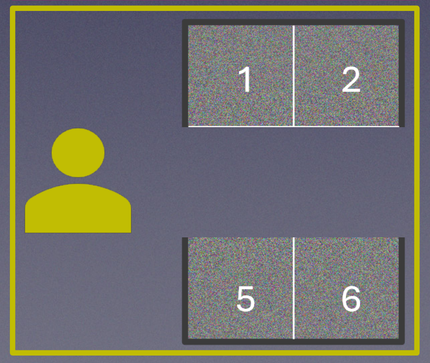


1	2
3	4
5	6

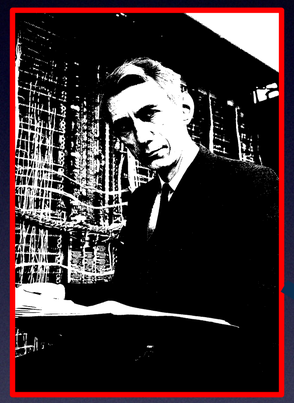






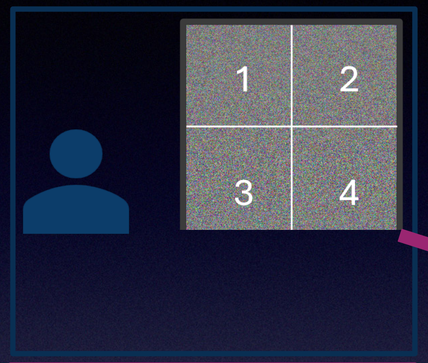


Rumore distribuito (condivisione del segreto)

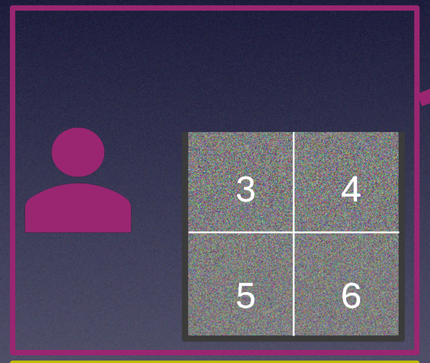


1	2
3	4
5	6

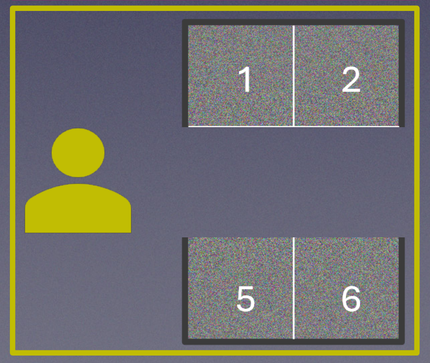




1	2
3	4



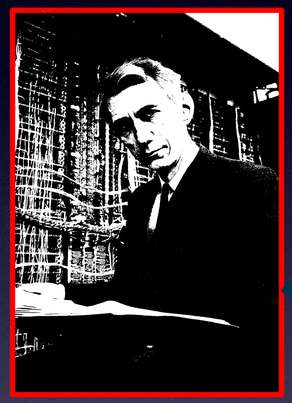
3	4
5	6



1	2
5	6

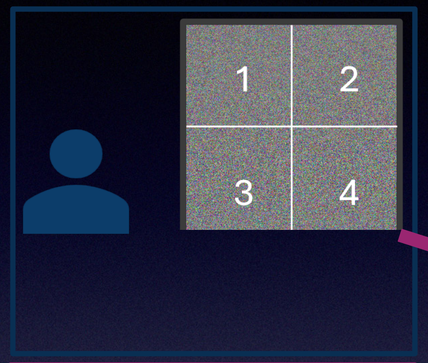
1	2
3	4
5	6

Rumore distribuito (condivisione del segreto)

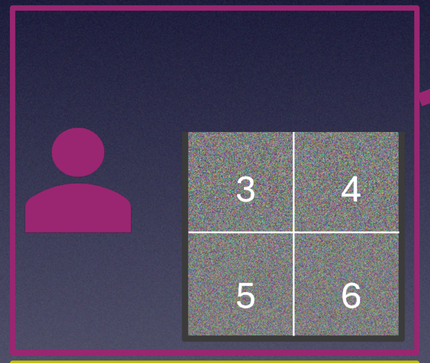


1	2
3	4
5	6

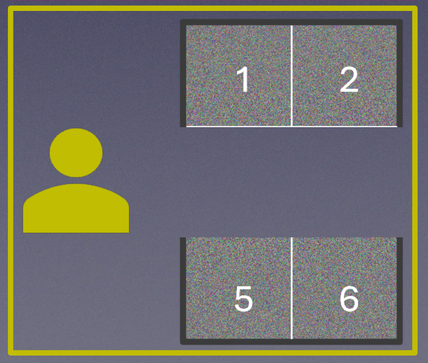




1	2
3	4

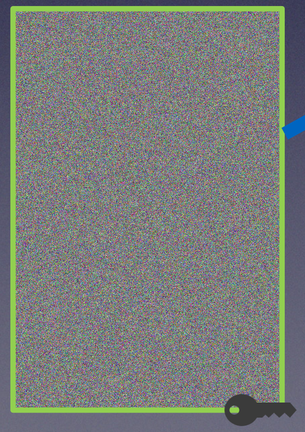


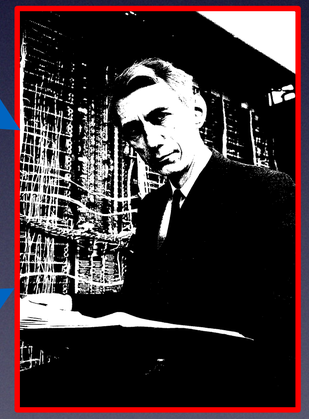
3	4
5	6



1	2
5	6

1	2
3	4
5	6





Varianti della malleabilità

Il concetto di rumore può essere declinato in molti modi

Varianti della malleabilità

Il concetto di rumore può essere declinato in molti modi

Verticale

Varianti della malleabilità

Il concetto di rumore può essere declinato in molti modi

Verticale

Orizzontale

Varianti della malleabilità

Il concetto di rumore può essere declinato in molti modi

Verticale

Orizzontale

La capacità di eliminare il rumore è distribuita verticalmente tra i partecipanti.

Il messaggio emerge solo collaborando.

Varianti della malleabilità

Il concetto di rumore può essere declinato in molti modi

Verticale

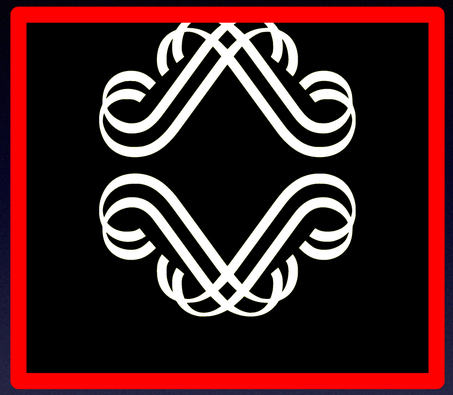
La capacità di eliminare il rumore è distribuita verticalmente tra i partecipanti.

Il messaggio emerge solo collaborando.

Orizzontale

Durante le operazioni sui testi cifrati, il rumore cresce insieme al messaggio, diffondendosi come una nube d'incertezza che deve essere contenuta.

Malleabilità
(Cifratura omomorfa)

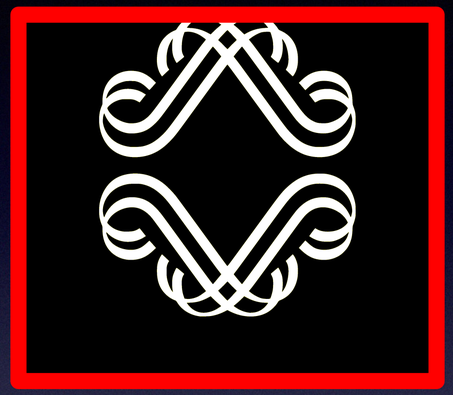


m_1

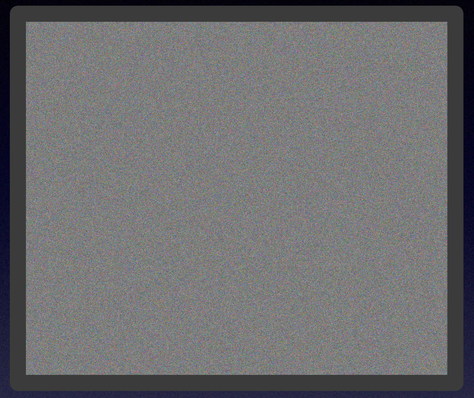
m_2



Malleabilità
(Cifratura omomorfa)



m_1

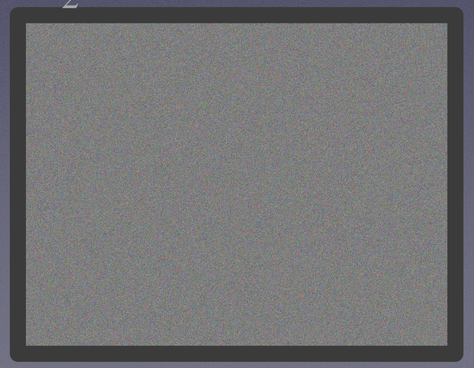


k_1

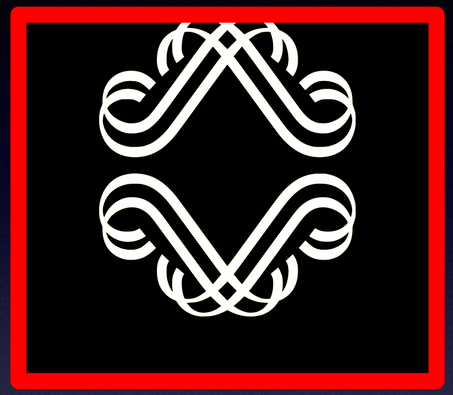
m_2



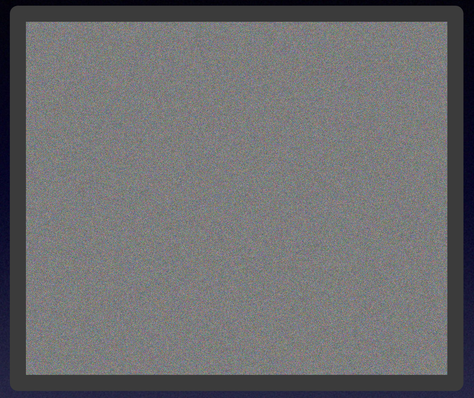
k_2



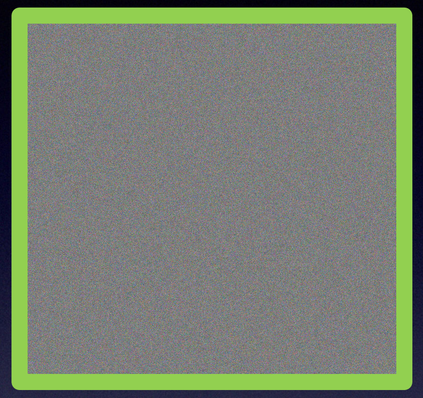
Malleabilità
(Cifratura omomorfa)



m_1



k_1

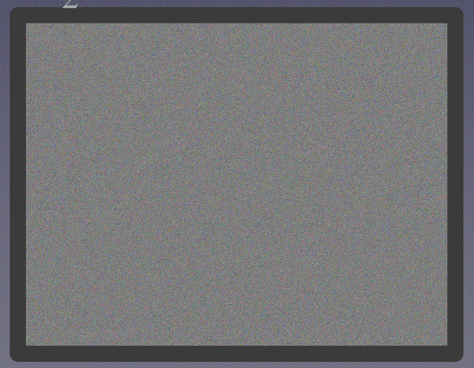


c_1

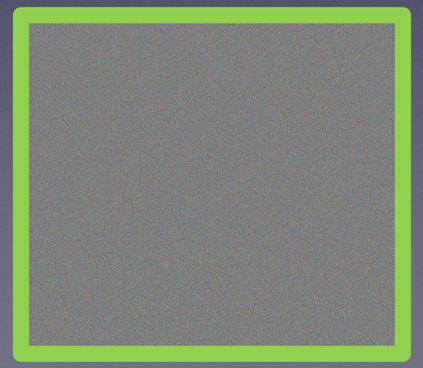
m_2



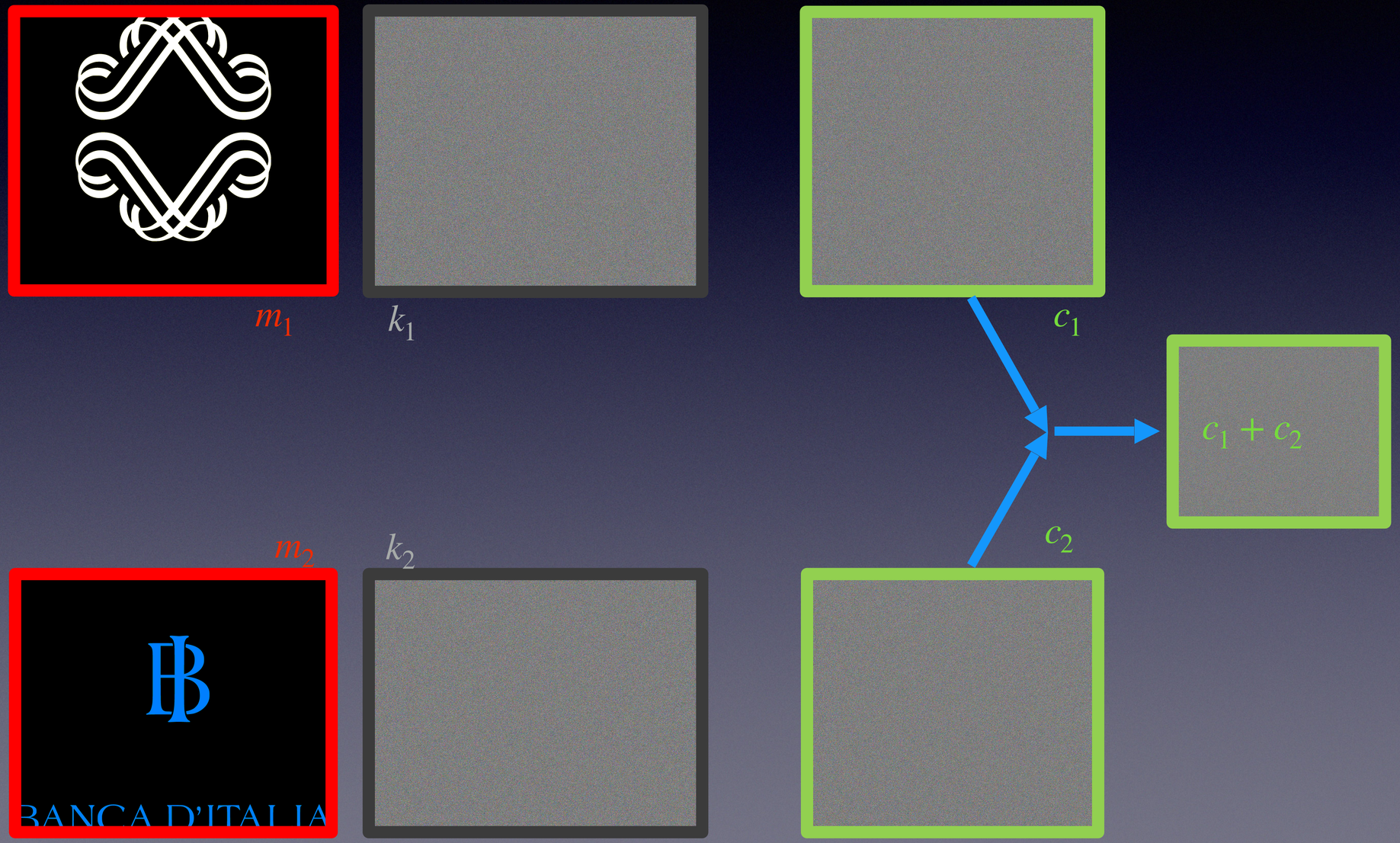
k_2



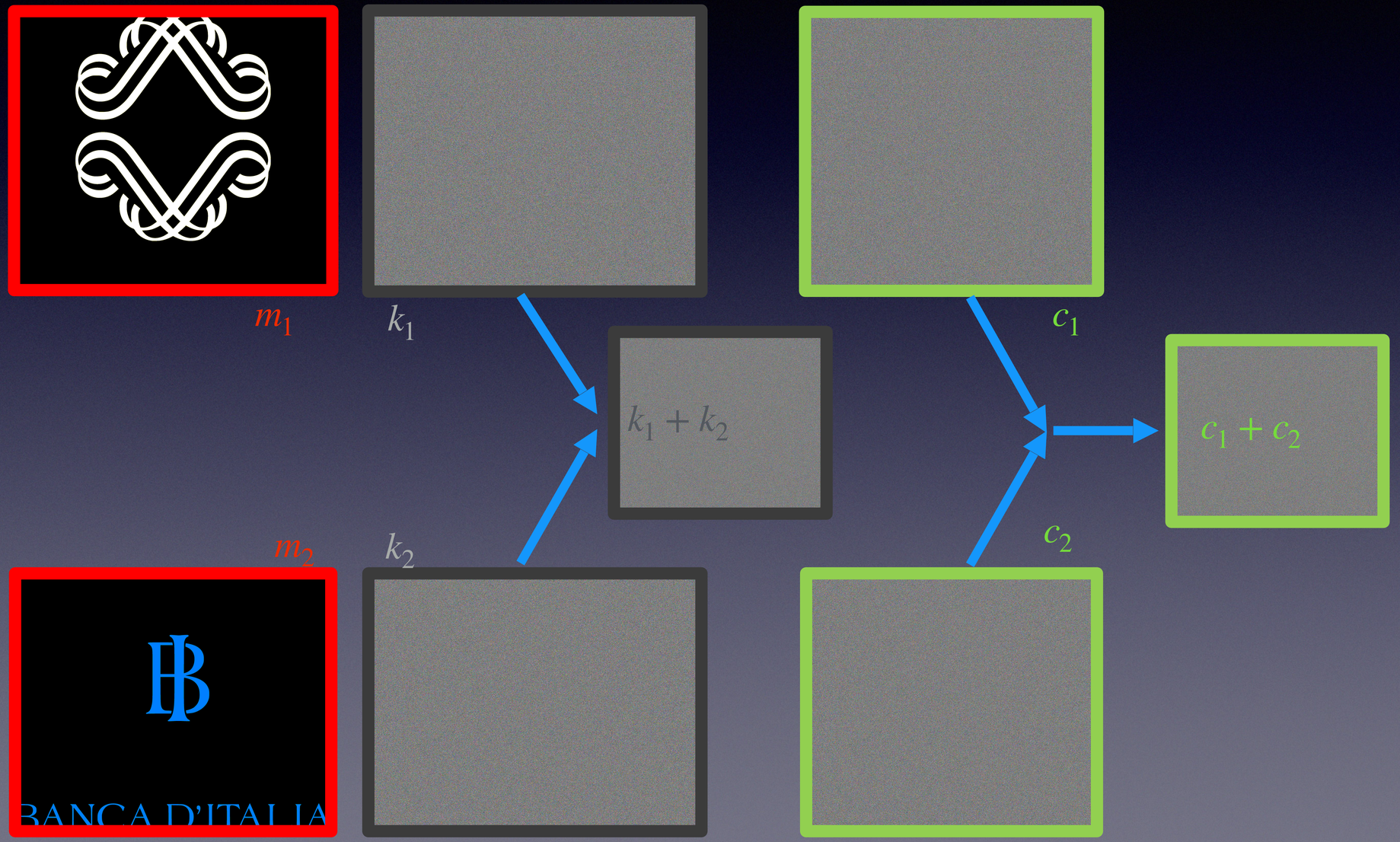
c_2



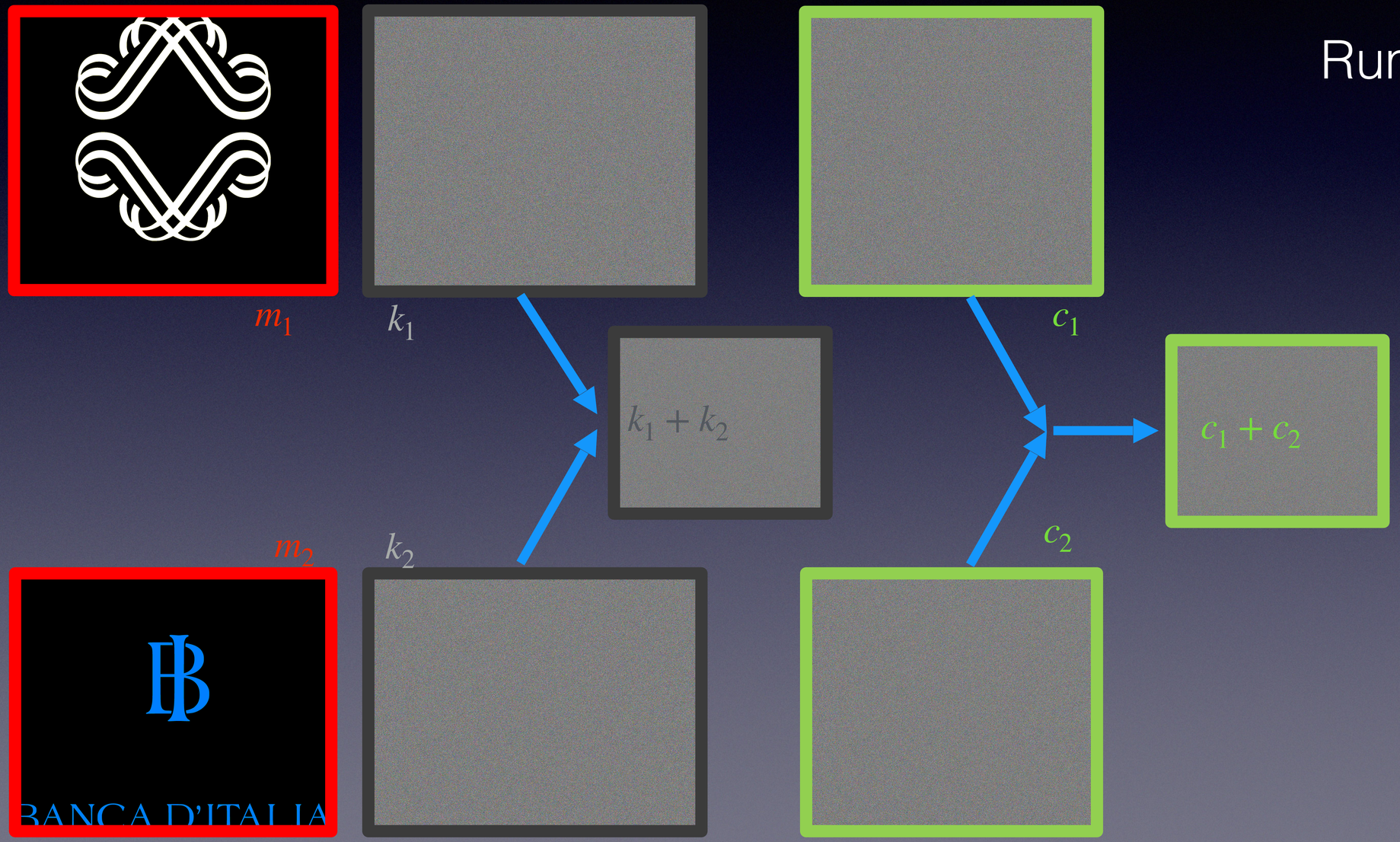
Malleabilità
(Cifratura omomorfa)



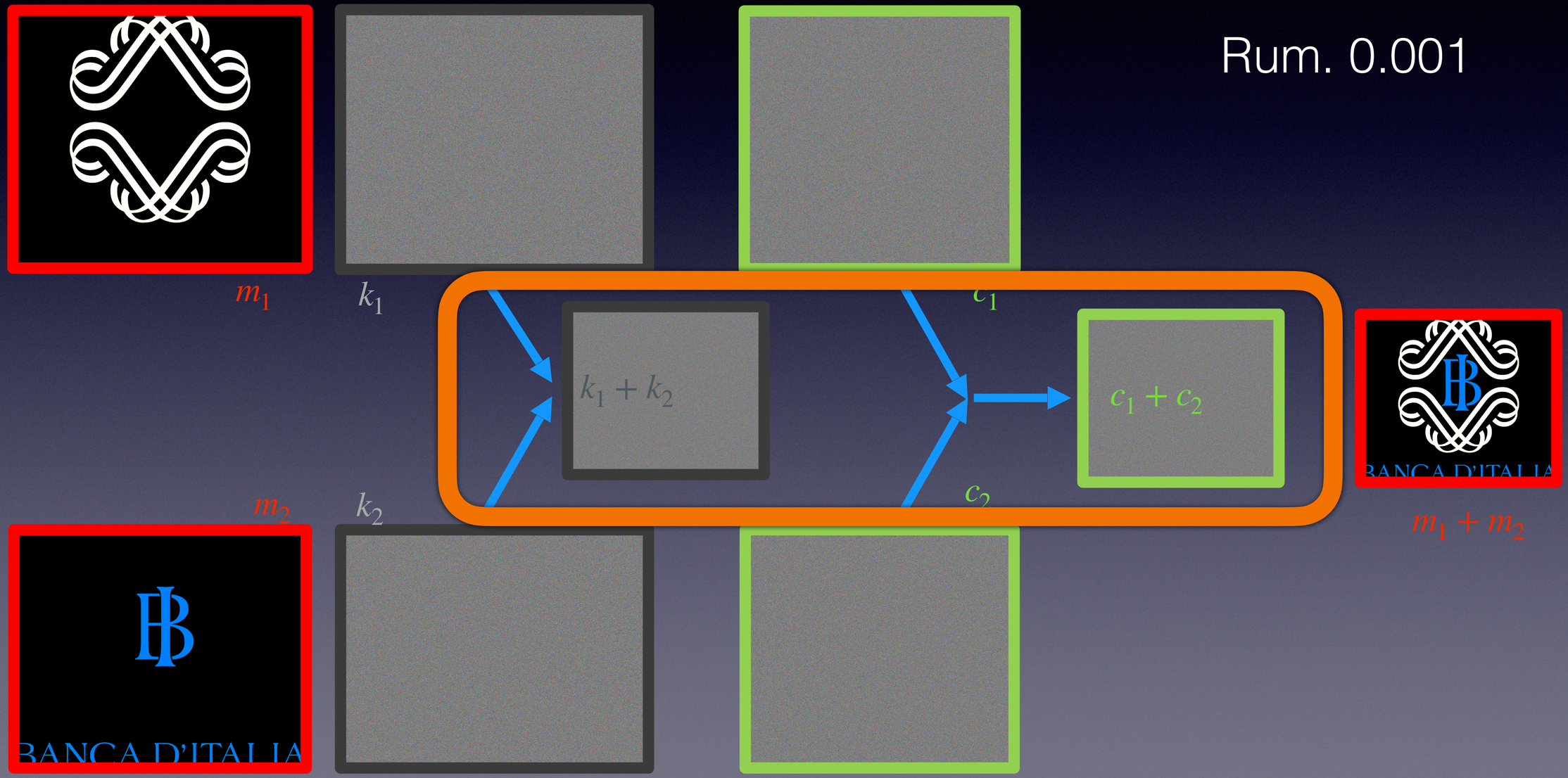
Malleabilità
(Cifratura omomorfa)



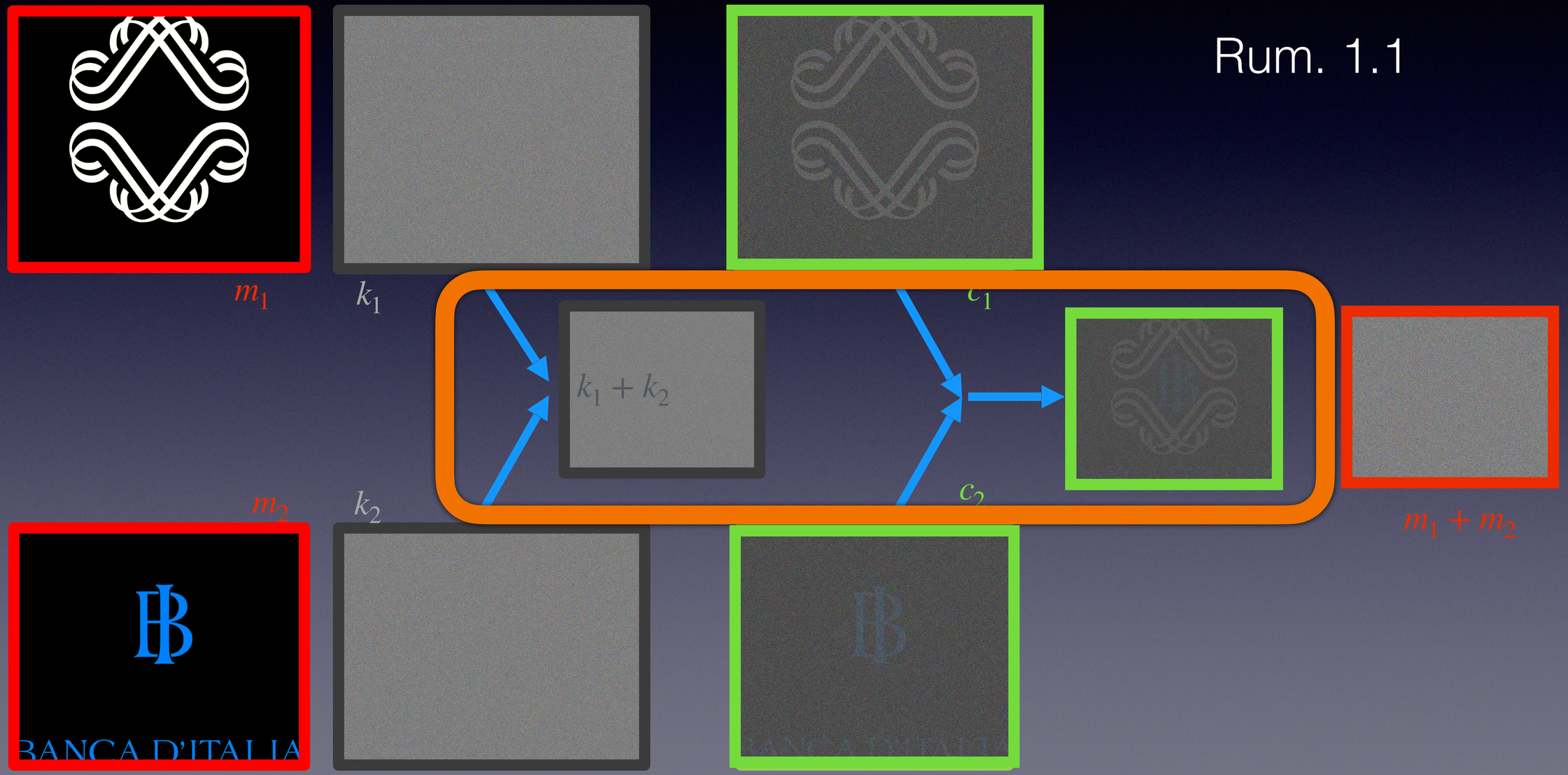
Malleabilità (Cifratura omomorfa)



Malleabilità
(Cifratura omomorfa)

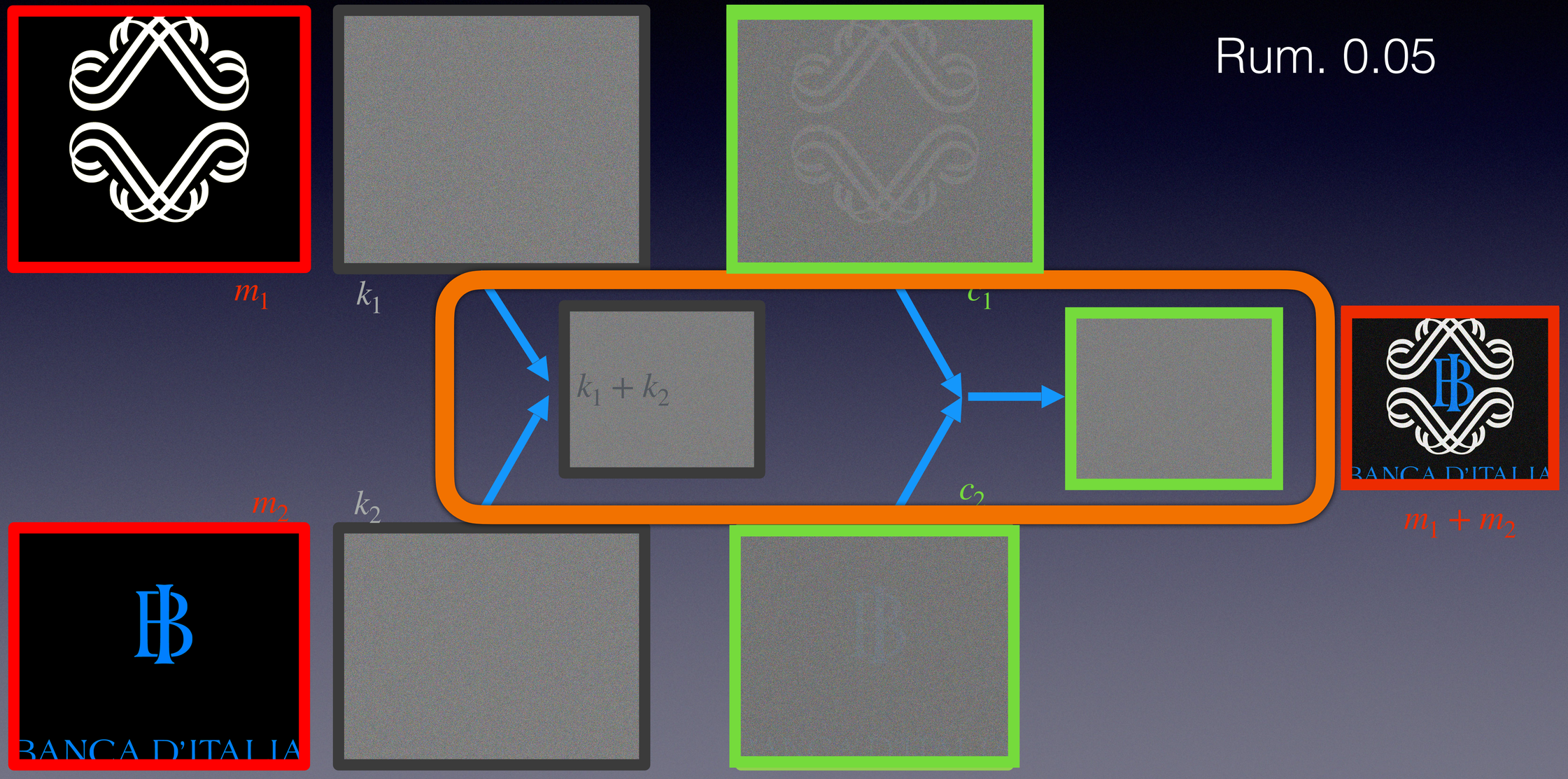


Malleabilità
(Cifratura omomorfa)

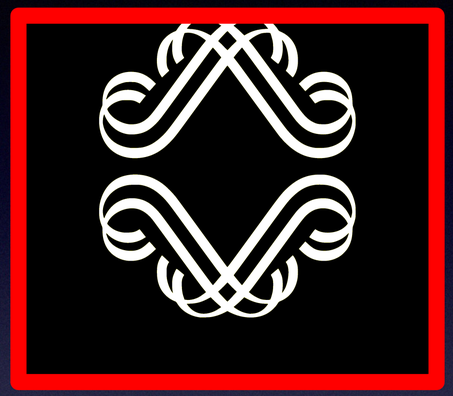


Rum. 1.1

Malleabilità
(Cifratura omomorfa)



Malleabilità



m_1



m_2



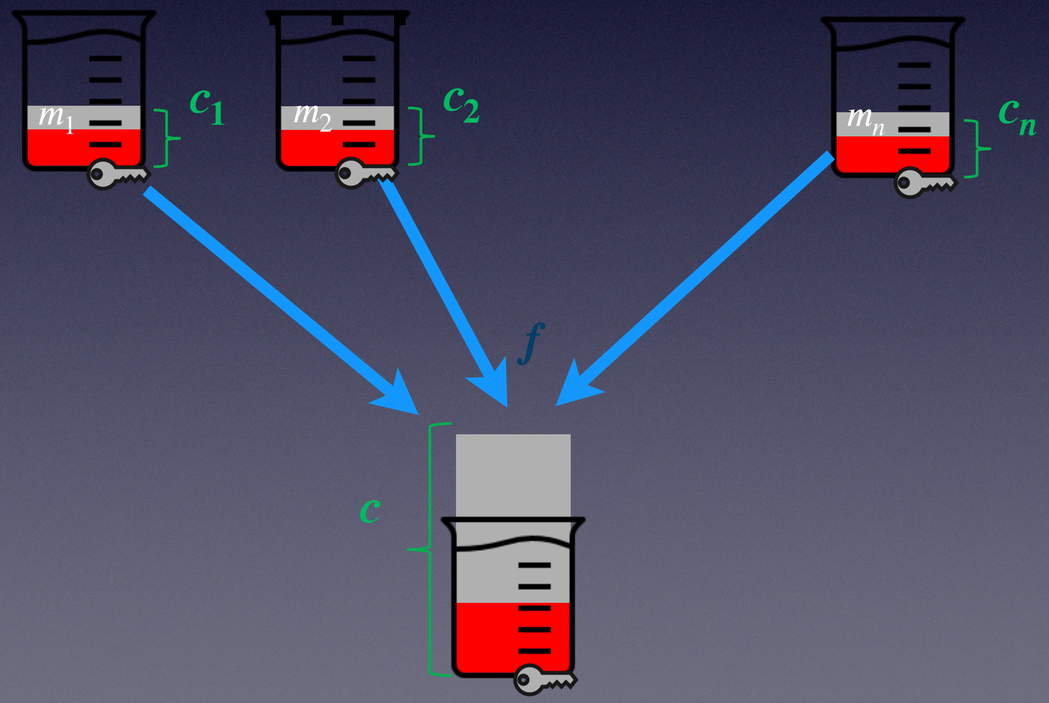


$+ m_2$

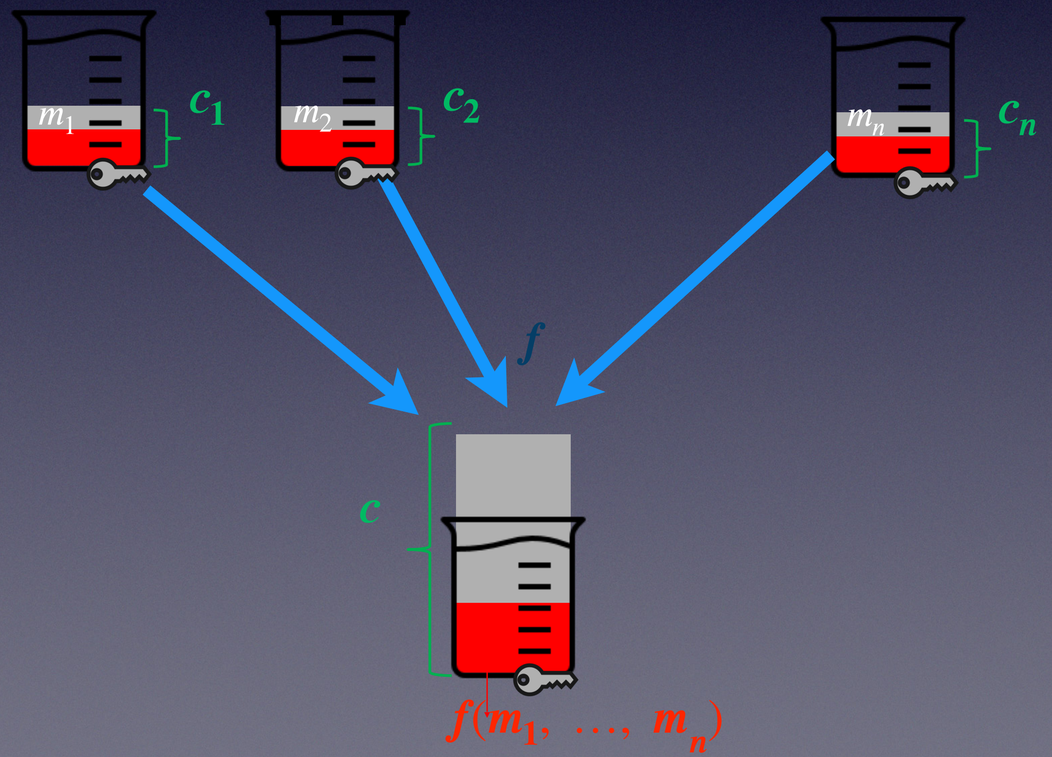
Bootstrap (crittografia)



Bootstrap (crittografia)



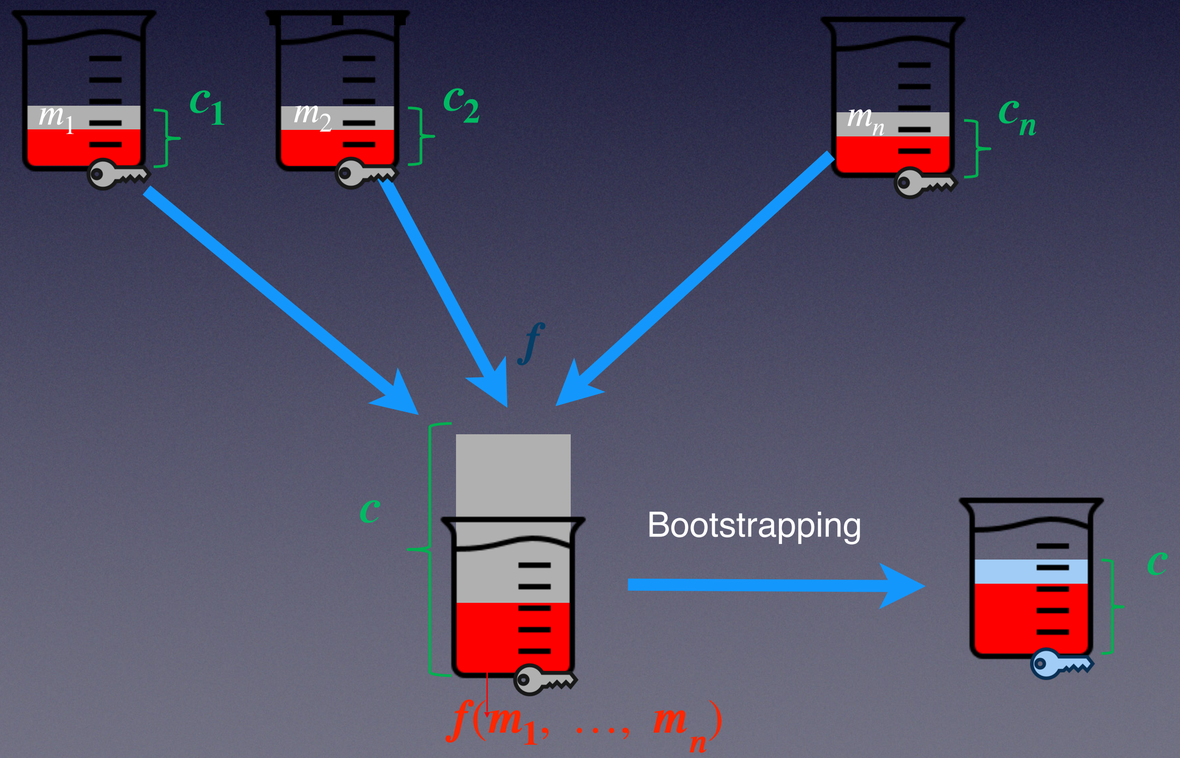
Bootstrap (crittografia)



Nella HE ogni operazione aumenta il rumore, rischiando di rendere inutilizzabile il testo cifrato.

Bootstrap (crittografia)

Il bootstrap crittografico è un reset controllato del rumore.
Permette di continuare a lavorare sui dati cifrati.



Nella HE ogni operazione aumenta il rumore, rischiando di rendere inutilizzabile il testo cifrato.

Cifratura omomorfa (HE)

Una banca usa un servizio cloud per calcolare il VaR del portafoglio.

I dati grezzi restano altamente sensibili.

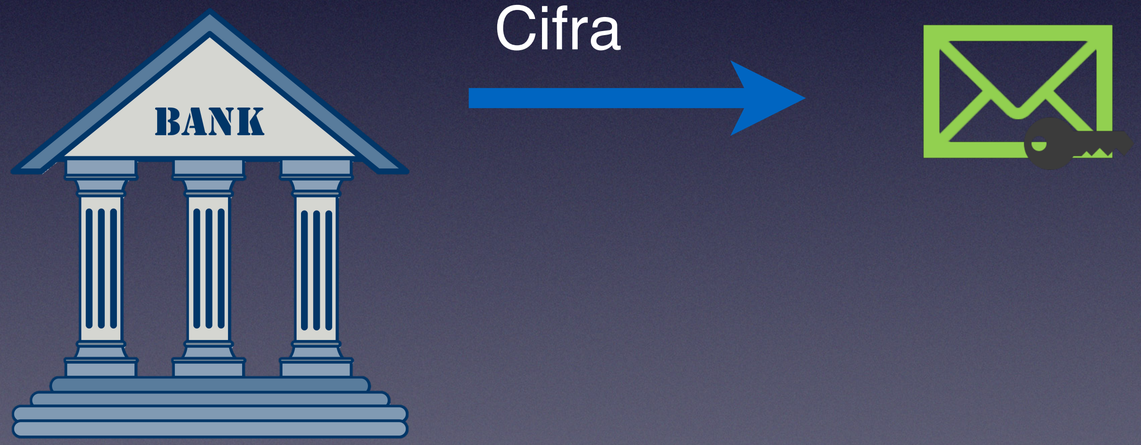


Banca

Cifratura omomorfa (HE)

Una banca usa un servizio cloud per calcolare il VaR del portafoglio.

I dati grezzi restano altamente sensibili.



Banca

Cifratura omomorfa (HE)

Una banca usa un servizio cloud per calcolare il VaR del portafoglio.

I dati grezzi restano altamente sensibili.



Cifra



Invia i dati cifrati



Banca

Provider cloud

Cifratura omomorfa (HE)

Una banca usa un servizio cloud per calcolare il VaR del portafoglio.

I dati grezzi restano altamente sensibili.



Banca

Cifra



Invia i dati cifrati



Restituisce i dati cifrati elaborati



Provider cloud

Cifratura omomorfa (HE)

Una banca usa un servizio cloud per calcolare il VaR del portafoglio.

I dati grezzi restano altamente sensibili.



Cifra



Invia i dati cifrati



Provider cloud

Restituisce i dati cifrati elaborati



Decifra

Banca

Cifratura omomorfa (HE)

Cifratura omomorfa (HE)

Consente calcoli su dati cifrati senza decifrarli.
I dati grezzi restano protetti.

Cifratura omomorfa (HE)

Consente calcoli su dati cifrati senza decifrarli.
I dati grezzi restano protetti.

FHE
Omomorfia completa

Qualsiasi operazione.

Cifratura omomorfa (HE)

Consente calcoli su dati cifrati senza decifrarli.
I dati grezzi restano protetti.

SHE
Omomorfia parziale

Operazioni aritmetiche limitate.

FHE
Omomorfia completa

Qualsiasi operazione.

Cifratura omomorfa (HE)

Consente calcoli su dati cifrati senza decifrarli.
I dati grezzi restano protetti.

SHE
Omomorfia parziale

Operazioni aritmetiche limitate.

FHE
Omomorfia completa

Qualsiasi operazione.

Spesso basta la SHE: scegliere lo strumento adatto al problema.

Cifratura omomorfa (HE)

Punti di forza	Punti deboli
Privacy	Carico computazionale
Calcolo su dati cifrati	Potenziale crescita della dimensione del testo cifrato
Nessun carico di comunicazione	Accumulo di rumore

Cifratura omomorfa (HE)

- **Privacy:** i dati rimangono cifrati durante l'intero calcolo.

Punti di forza	Punti deboli
Privacy	Carico computazionale
Calcolo su dati cifrati	Potenziale crescita della dimensione del testo cifrato
Nessun carico di comunicazione	Accumulo di rumore

Cifratura omomorfa (HE)

- **Privacy:** i dati rimangono cifrati durante l'intero calcolo.
- **Calcolo su dati cifrati:** consente l'elaborazione senza esporre i dati effettivi.

Punti di forza	Punti deboli
Privacy	Carico computazionale
Calcolo su dati cifrati	Potenziale crescita della dimensione del testo cifrato
Nessun carico di comunicazione	Accumulo di rumore

Cifratura omomorfa (HE)

- **Privacy:** i dati rimangono cifrati durante l'intero calcolo.
- **Calcolo su dati cifrati:** consente l'elaborazione senza esporre i dati effettivi.
- **Correttezza del calcolo:** le operazioni sui dati cifrati producono risultati che, una volta decifrati, sono corretti ed equivalenti ai calcoli sui dati in chiaro.

Punti di forza	Punti deboli
Privacy	Carico computazionale
Calcolo su dati cifrati	Potenziale crescita della dimensione del testo cifrato
Nessun carico di comunicazione	Accumulo di rumore

Cifratura omomorfa (HE)

- **Privacy:** i dati rimangono cifrati durante l'intero calcolo.
- **Calcolo su dati cifrati:** consente l'elaborazione senza esporre i dati effettivi.
- **Correttezza del calcolo:** le operazioni sui dati cifrati producono risultati che, una volta decifrati, sono corretti ed equivalenti ai calcoli sui dati in chiaro.
- **Decifratura lato client:** nessuna parte intermedia può accedere alle informazioni sensibili.

Punti di forza	Punti deboli
Privacy	Carico computazionale
Calcolo su dati cifrati	Potenziale crescita della dimensione del testo cifrato
Nessun carico di comunicazione	Accumulo di rumore

Cifratura omomorfa (HE)

- **Privacy:** i dati rimangono cifrati durante l'intero calcolo.
- **Calcolo su dati cifrati:** consente l'elaborazione senza esporre i dati effettivi.
- **Correttezza del calcolo:** le operazioni sui dati cifrati producono risultati che, una volta decifrati, sono corretti ed equivalenti ai calcoli sui dati in chiaro.
- **Decifratura lato client:** nessuna parte intermedia può accedere alle informazioni sensibili.
- **Non interattivo:** il server può eseguire calcoli senza interagire continuamente con il proprietario dei dati.

Punti di forza	Punti deboli
Privacy	Carico computazionale
Calcolo su dati cifrati	Potenziale crescita della dimensione del testo cifrato
Nessun carico di comunicazione	Accumulo di rumore

Computazione a parti multiple sicuro (SMPC)



HE consente calcoli su dati cifrati con la stessa chiave.









Banche che stimano congiuntamente il rischio sistemico senza rivelare i dati grezzi

Computazione a parti multiple sicuro (SMPC)



HE consente calcoli su dati cifrati con la stessa chiave.









Banche che stimano congiuntamente il rischio sistemico senza rivelare i dati grezzi

Computazione a parti multiple sicuro (SMPC)



HE consente calcoli su dati cifrati con la stessa chiave.

E se…









Banche che stimano congiuntamente il rischio sistemico senza rivelare i dati grezzi

Computazione a parti multiple sicuro (SMPC)



HE consente calcoli su dati cifrati con la stessa chiave.

E se…







parti diverse potessero calcolare congiuntamente funzioni complesse sui propri dati



Banche che stimano congiuntamente il rischio sistemico senza rivelare i dati grezzi

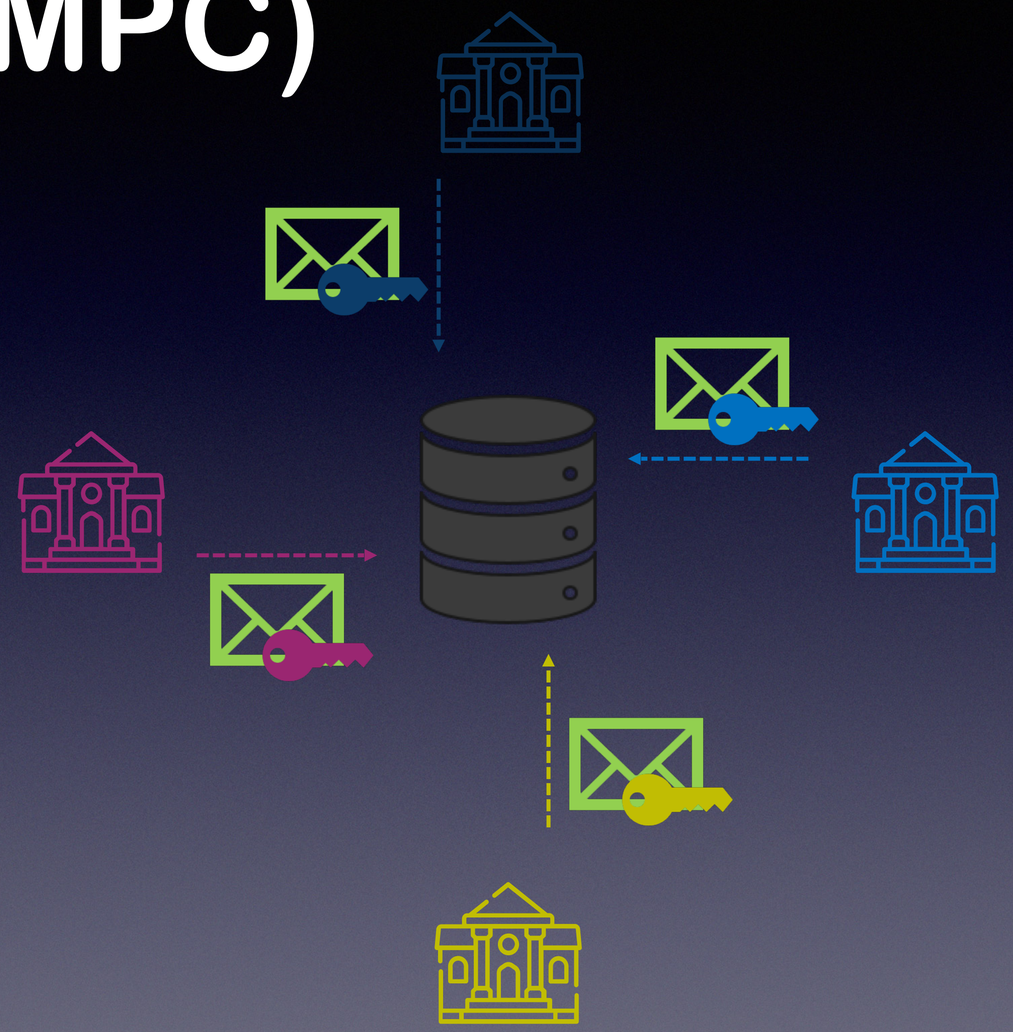
Computazione a parti multiple sicuro (SMPC)

HE consente calcoli su dati cifrati con la stessa chiave.

E se…

parti diverse potessero calcolare congiuntamente funzioni complesse sui propri dati

senza mai rivelare i dati grezzi?



Banche che stimano congiuntamente il rischio sistemico senza rivelare i dati grezzi

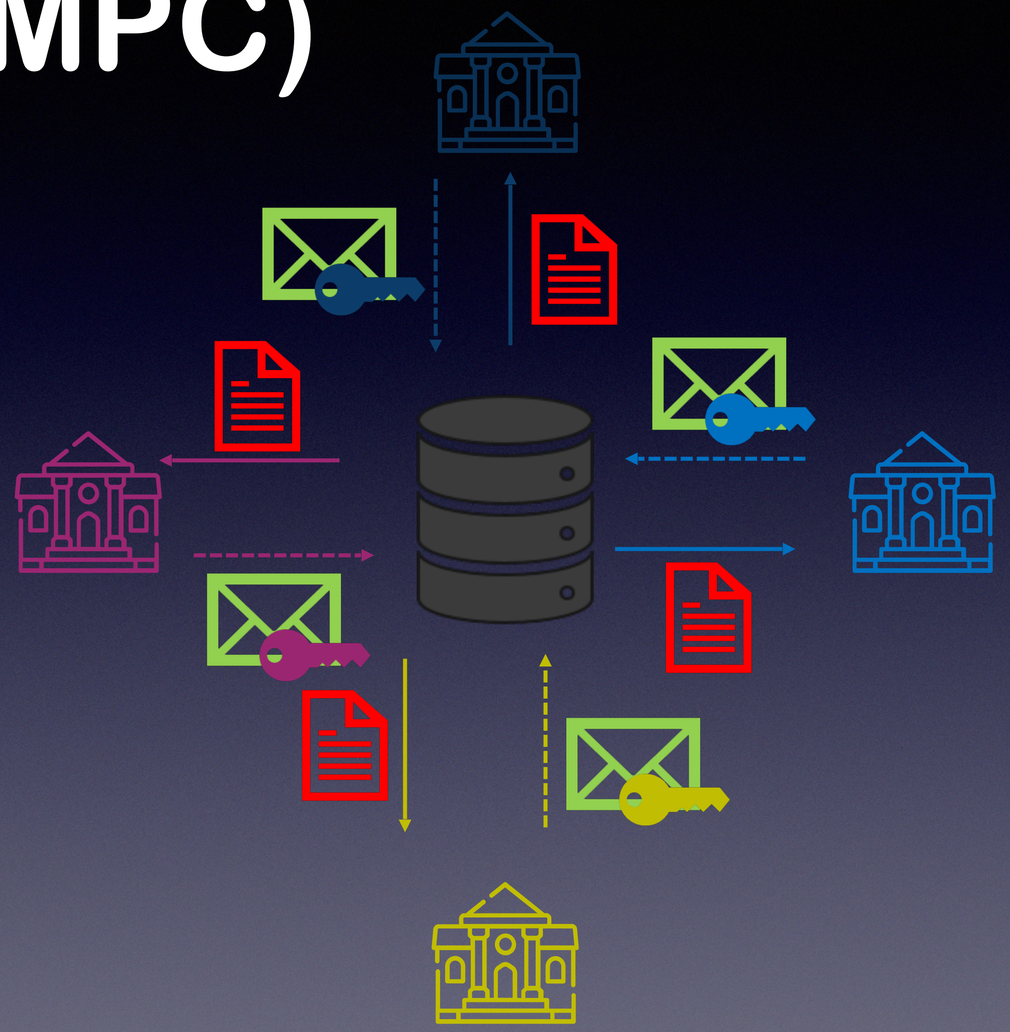
Computazione a parti multiple sicuro (SMPC)

HE consente calcoli su dati cifrati con la stessa chiave.

E se…

parti diverse potessero calcolare congiuntamente funzioni complesse sui propri dati

senza mai rivelare i dati grezzi?



Banche che stimano congiuntamente il rischio sistemico senza rivelare i dati grezzi

Calcolo a parti multiple sicuro (SMPC)

WHO IS RICHER?

BOB **ALICE**



Yao’s Millionaires’ Problem, 1982

Calcolo a parti multiple sicuro (SMPC)

WHO IS RICHER?

CARATTERISTICHE

BOB **ALICE**



Yao’s Millionaires’ Problem, 1982

Calcolo a parti multiple sicuro (SMPC)

WHO IS RICHER?

BOB **ALICE**



Yao’s Millionaires’ Problem, 1982

CARATTERISTICHE

Privacy – ogni parte apprende solo il proprio risultato.

Calcolo a parti multiple sicuro (SMPC)

WHO IS RICHER?

BOB **ALICE**



Yao’s Millionaires’ Problem, 1982

CARATTERISTICHE

Privacy – ogni parte apprende solo il proprio risultato.

Correttezza – i risultati restano corretti anche in presenza di avversari.

Calcolo a parti multiple sicuro (SMPC)

WHO IS RICHER?

BOB **ALICE**



Yao’s Millionaires’ Problem, 1982

CARATTERISTICHE

Privacy – ogni parte apprende solo il proprio risultato.

Correttezza – i risultati restano corretti anche in presenza di avversari.

Input indipendenti – nessuna parte adatta i propri input agli altri.

Calcolo a parti multiple sicuro (SMPC)

WHO IS RICHER?

BOB **ALICE**



Yao’s Millionaires’ Problem, 1982

CARATTERISTICHE

Privacy – ogni parte apprende solo il proprio risultato.

Correttezza – i risultati restano corretti anche in presenza di avversari.

Input indipendenti – nessuna parte adatta i propri input agli altri.

Consegna garantita – gli avversari non bloccano i risultati.

Calcolo a parti multiple sicuro (SMPC)

WHO IS RICHER?

BOB **ALICE**



Yao’s Millionaires’ Problem, 1982

CARATTERISTICHE

Privacy – ogni parte apprende solo il proprio risultato.

Correttezza – i risultati restano corretti anche in presenza di avversari.

Input indipendenti – nessuna parte adatta i propri input agli altri.

Consegna garantita – gli avversari non bloccano i risultati.

Equità – tutti ricevono i risultati nello stesso momento.

FHE e SMPC

ASPETTO	CIFRATURA OMOMORFA	CALCOLO A PARTI MULTIPLE SICURO
Idea di base	Calcolo su testi cifrati	Calcolo con segreti condivisi
Riservatezza dei dati	I dati restano cifrati	Nessuna parte vede l'intero input
Dove si calcola	Server/cloud unico	Tra le parti
Comunicazione	Basso	Alto
Calcolo	Moderato-alto (schema HE)	Moderato-alto (n. parti)

FHE e SMPC



Sono complementari.

Non rivali, ma due strumenti nella stessa cassetta degli attrezzi.

ASPETTO	CIFRATURA OMOMORFA	CALCOLO A PARTI MULTIPLE SICURO
Idea di base	Calcolo su testi cifrati	Calcolo con segreti condivisi
Riservatezza dei dati	I dati restano cifrati	Nessuna parte vede l'intero input
Dove si calcola	Server/cloud unico	Tra le parti
Comunicazione	Basso	Alto
Calcolo	Moderato-alto (schema HE)	Moderato-alto (n. parti)

Prova a conoscenza zero (ZKP)

Prova a conoscenza zero (ZKP)

Una banca vuole dimostrare di disporre di riserve sufficienti senza divulgare il proprio bilancio dettagliato.

Prova a conoscenza zero (ZKP)

Una banca vuole dimostrare di disporre di riserve sufficienti senza divulgare il proprio bilancio dettagliato.

Prova a conoscenza zero (ZKP)

Una banca vuole dimostrare di disporre di riserve sufficienti senza divulgare il proprio bilancio dettagliato.

Oppure un investitore vuole dimostrare la conformità a determinati requisiti senza esporre i propri conti.

Prova a conoscenza zero (ZKP)

Una banca vuole dimostrare di disporre di riserve sufficienti senza divulgare il proprio bilancio dettagliato.

Oppure un investitore vuole dimostrare la conformità a determinati requisiti senza esporre i propri conti.

Prova a conoscenza zero (ZKP)

Una banca vuole dimostrare di disporre di riserve sufficienti senza divulgare il proprio bilancio dettagliato.

Oppure un investitore vuole dimostrare la conformità a determinati requisiti senza esporre i propri conti.

Una prova a conoscenza zero consente a una parte di dimostrare un'affermazione senza rivelare alcuna informazione aggiuntiva.

Prova a conoscenza zero (ZKP)

Una banca vuole dimostrare di disporre di riserve sufficienti senza divulgare il proprio bilancio dettagliato.

Oppure un investitore vuole dimostrare la conformità a determinati requisiti senza esporre i propri conti.

Una prova a conoscenza zero consente a una parte di dimostrare un'affermazione senza rivelare alcuna informazione aggiuntiva.



Privacy

Machine Learning (ML) è ampiamente utilizzato nella data analysis.
Comunque, ad ogni livello della elaborazione con il ML emerge un punto di attenzione critica:



Training dataset **Model** **Prompts and response**

Privacy

Machine Learning (ML) è ampiamente utilizzato nella data analysis.
Comunque, ad ogni livello della elaborazione con il ML emerge un punto di attenzione critica:



Training dataset | **Model** | **Prompts and response**

In fase di addestramento del modello si vogliono garanzie sulla privacy dei dati utilizzati:
Differential Privacy.

se diverse istituzioni vogliono collaborare:
Federated Learning.

Privacy

Machine Learning (ML) è ampiamente utilizzato nella data analysis.
Comunque, ad ogni livello della elaborazione con il ML emerge un punto di attenzione critica:

Training dataset

In fase di addestramento del modello si vogliono garanzie sulla privacy dei dati utilizzati:
Differential Privacy.

se diverse istituzioni vogliono collaborare:
Federated Learning.

Model

Se si vogliono proteggere i pesi del modello:

Homomorphic Encryption.

Prompts and response

Privacy

Machine Learning (ML) è ampiamente utilizzato nella data analysis.
Comunque, ad ogni livello della elaborazione con il ML emerge un punto di attenzione critica:

Training dataset

In fase di addestramento del modello si vogliono garanzie sulla privacy dei dati utilizzati:
Differential Privacy.

se diverse istituzioni vogliono collaborare:
Federated Learning.

Model

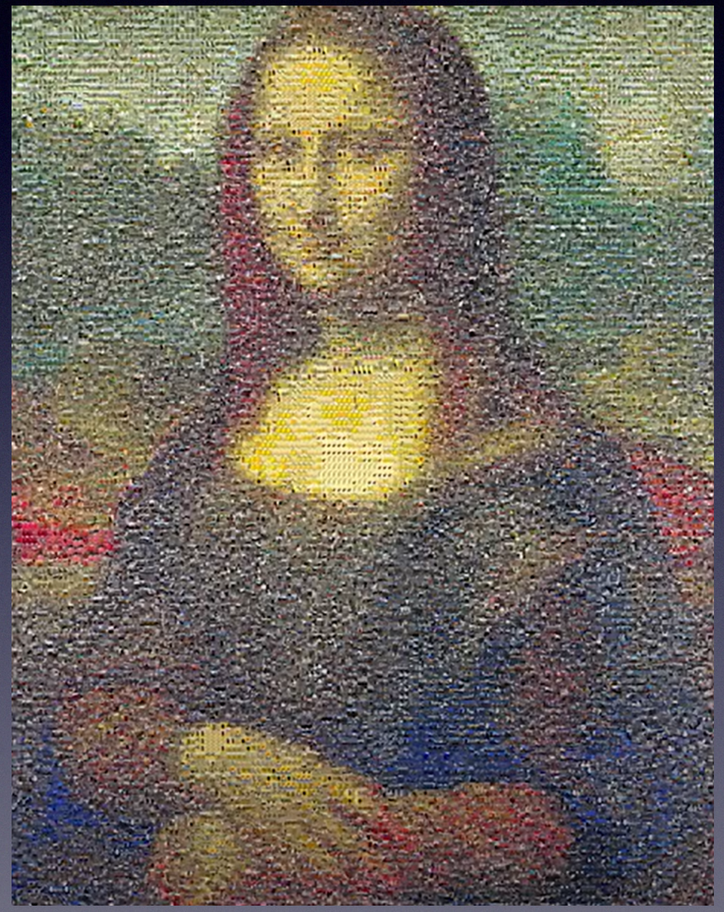
Se si vogliono proteggere i pesi del modello:

Homomorphic Encryption.

Prompts and response

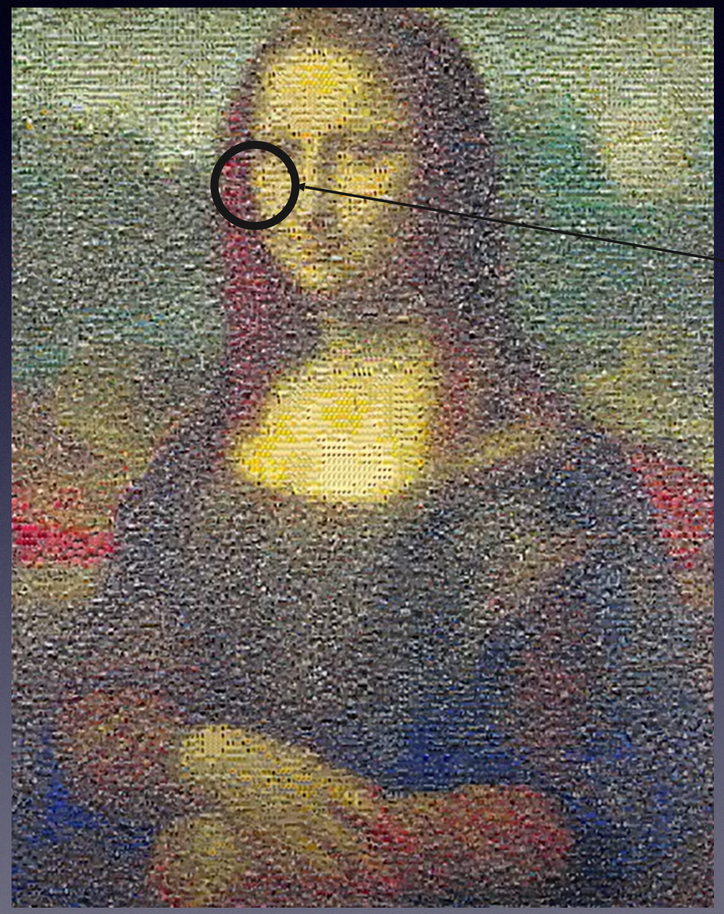
Se si vogliono proteggere I prompts dell'utente e le risposte dell'AI: serve un canale sicuro come nella **End-to-End Encryption**, Eventualmente combinata con
advanced cryptographic techniques.

Differential Privacy (DP)



Source: Differential Privacy on PyTorch I PyTorch Developer Day 2020

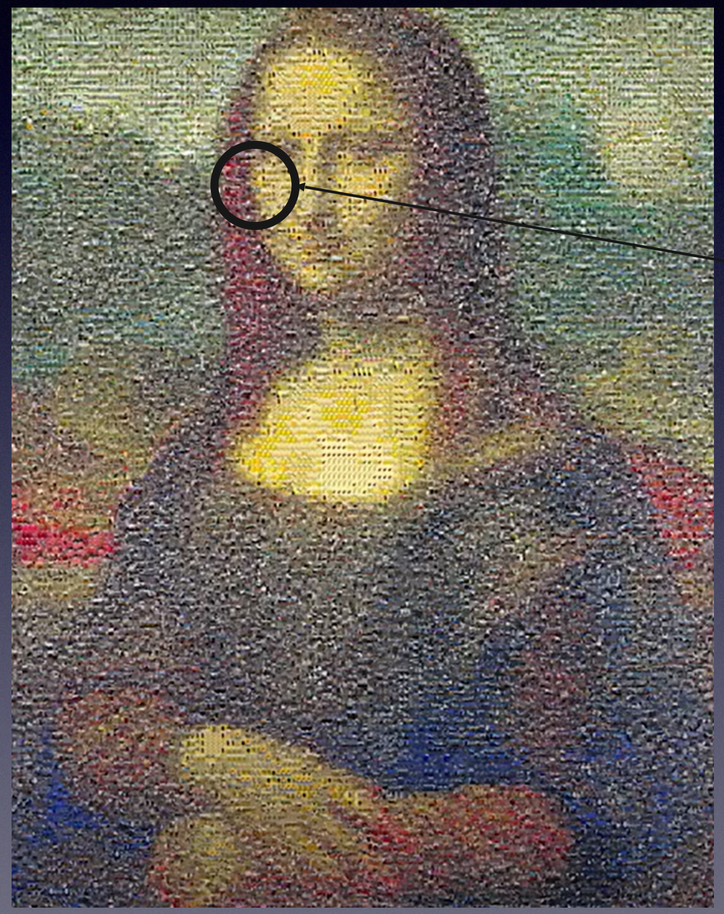
Differential Privacy (DP)





Source: Differential Privacy on PyTorch I PyTorch Developer Day 2020

Differential Privacy (DP)

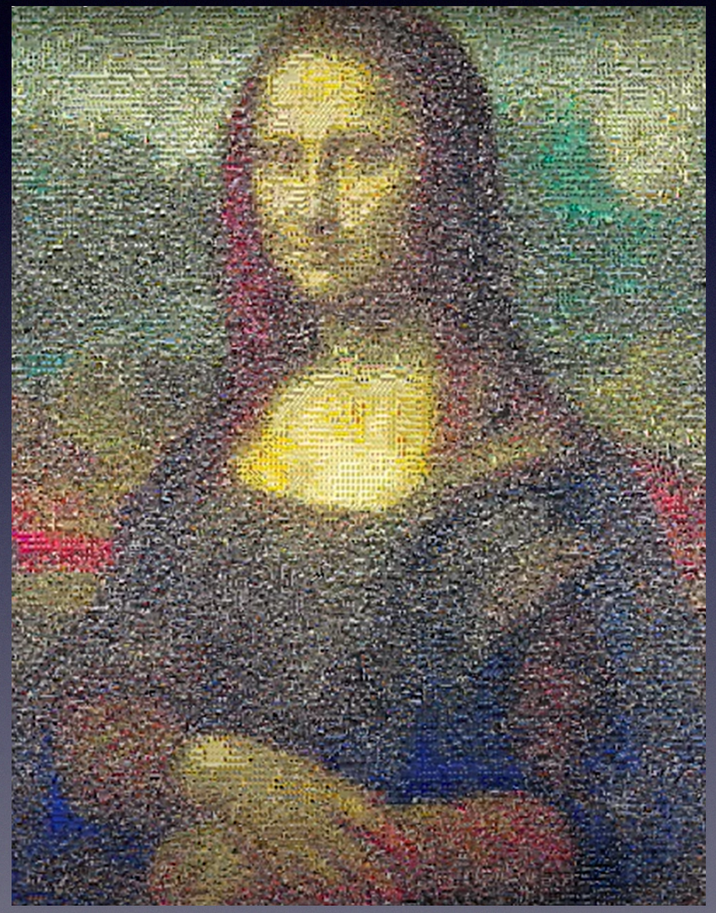




Source: Differential Privacy on PyTorch I PyTorch Developer Day 2020

Senza protezione, lo zoom a livello del dato rivela l’identità del singolo.

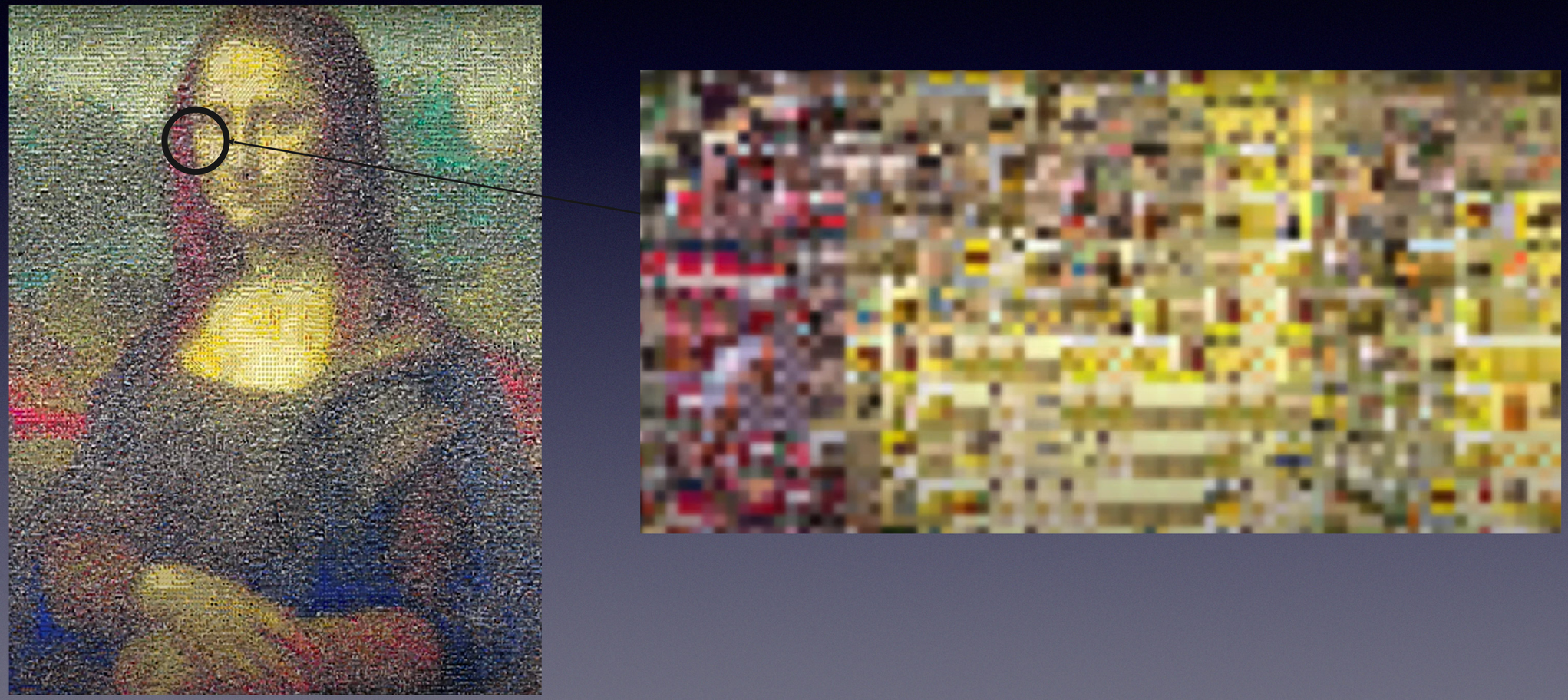
Differential Privacy (DP)



Source: Differential Privacy on PyTorch I PyTorch Developer Day 2020

https://www.census.gov/library/video/2019/protecting-privacy.html

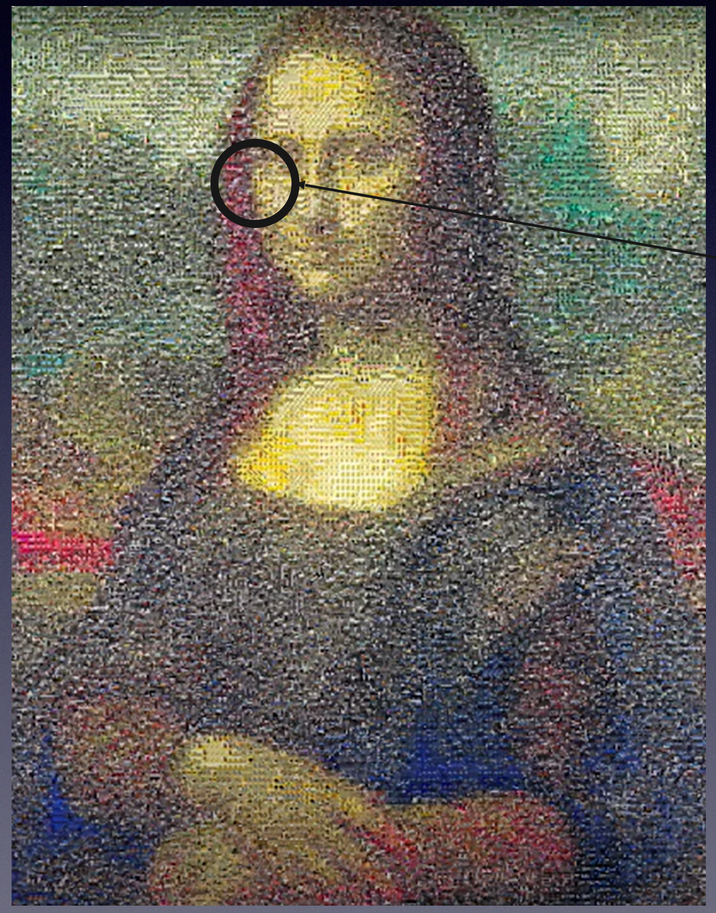
Differential Privacy (DP)



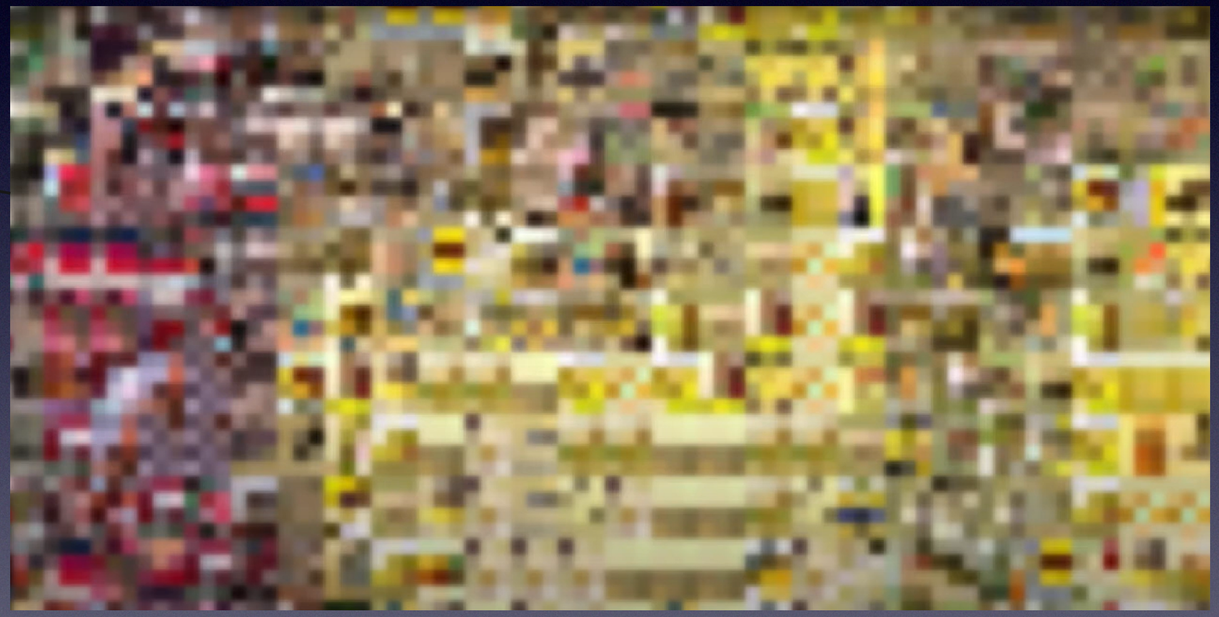
Source: Differential Privacy on PyTorch I PyTorch Developer Day 2020

https://www.census.gov/library/video/2019/protecting-privacy.html

Differential Privacy (DP)



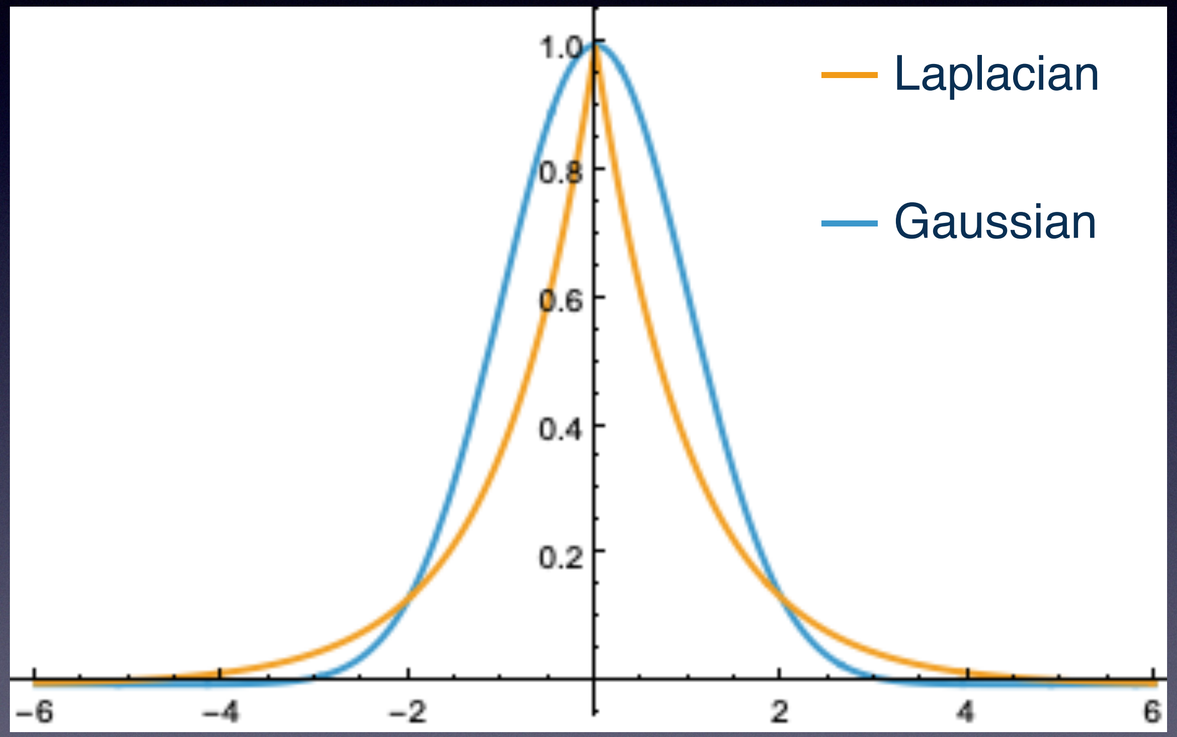
Source: Differential Privacy on PyTorch I PyTorch Developer Day 2020



Aggiungendo rumore
la figura resta globalmente comprensibile mentre se andiamo a guardare i singoli dettagli non riusciamo più a capire di cosa si tratta

https://www.census.gov/library/video/2019/protecting-privacy.html

Che tipo di rumore?



Il **rumore Gaussiano** non sempre va bene. Delle volte lascia spazio a **information leakage.**

Il **rumore Laplaciano** viene preferito nella DP, perché ha “heavier tails”.

Per questo garantisce differenze tra i database vengono mascherate in maniera più robusta.

Grazie per l’attenzione!

ci sono domande ?

Queste slides sono un adattamento della presentazione in collaborazione con **Carla Mascia** di DataKrypto alla First international conference: Financial Cryptography in Rome -- Centro Convegni "Carlo A. Ciampi", Banca d'Italia, Rome (IT) dal titolo: **Cryptographic algorithms and protocols for financial data analysis** October 1st, 2025. link