

Crittografia e Crittotecnologie

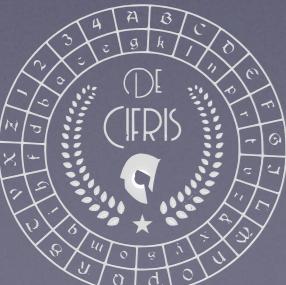
Marco Pedicini



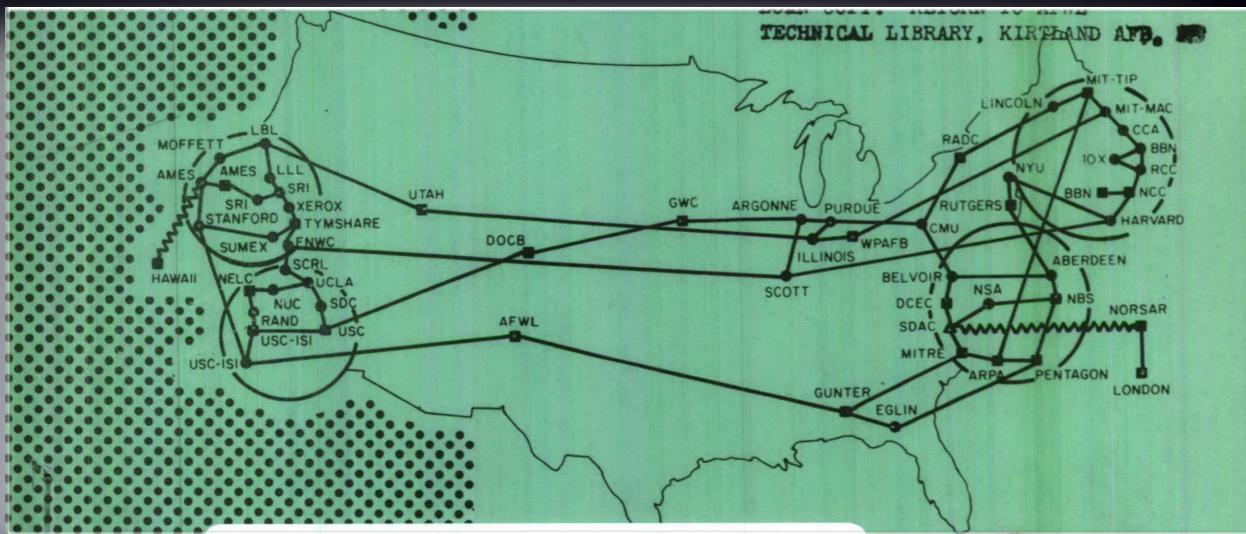
De Cifris Incontra Perugia
16.10.2019

Abstract

Il recente sviluppo scientifico e tecnologico ha avuto un impatto in tutti i campi della conoscenza ed ha trasformato anche la crittografia ampliandone il raggio di azione: dai compiti di protezione della comunicazione sono stati derivati nuovi paradigmi che rendono applicabili molte nuove metodologie per rispondere al meglio alle mutate esigenze di sicurezza: la riservatezza in ambito distribuito (cifratura omomorfa), senza bisogno di entità centralizzate (blockchain), la scalabilità al livello planetario (cloud computing), l'utilizzo di proprietà biometriche per l'autenticazione. Mostreremo alcuni dei passaggi fondamentali che hanno abilitato questi nuovi scenari.

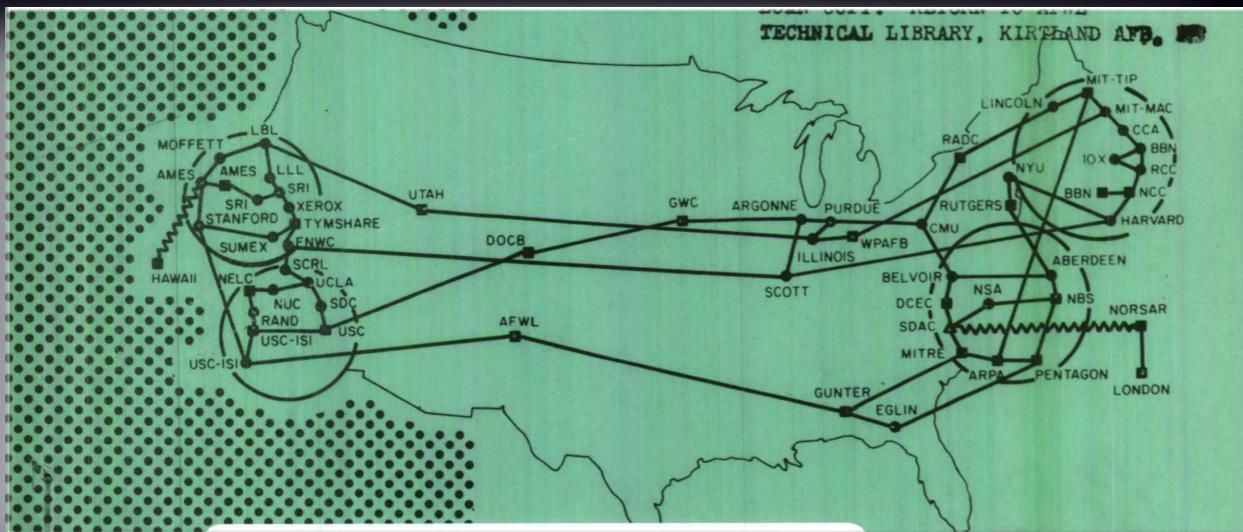


Infrastruttura di comunicazione



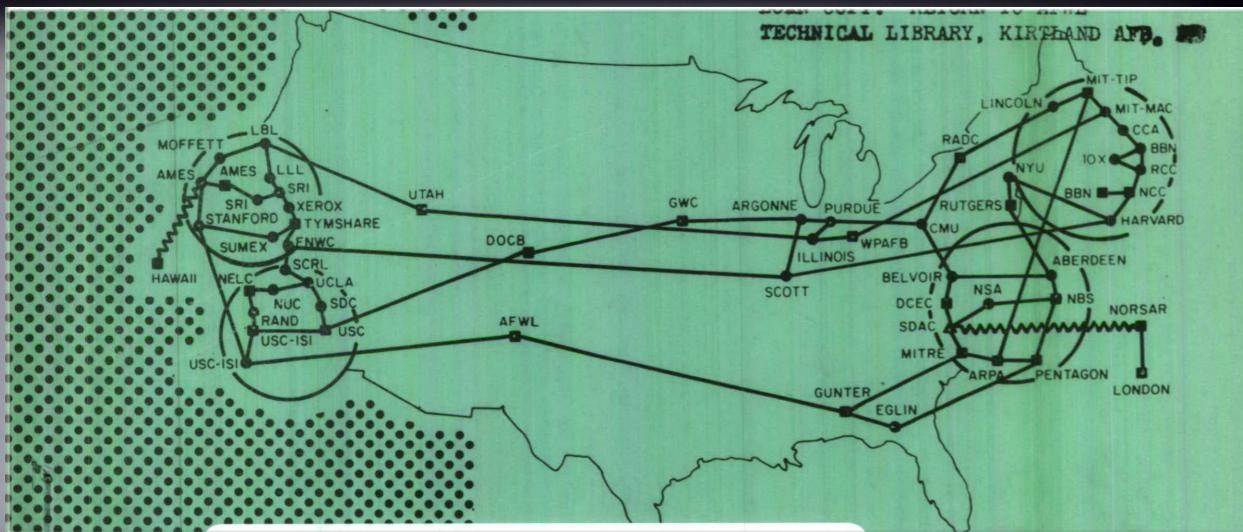
Infrastruttura di comunicazione

- Oggi tutti riconoscono questa immagine ([hint](#))

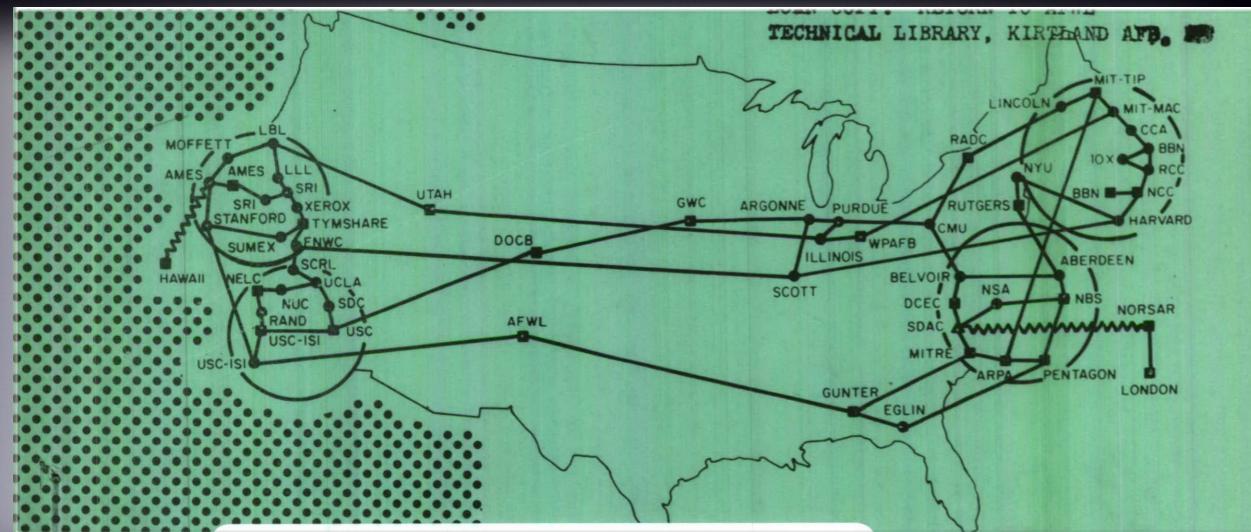


Infrastruttura di comunicazione

- Oggi tutti riconoscono questa immagine ([hint](#))



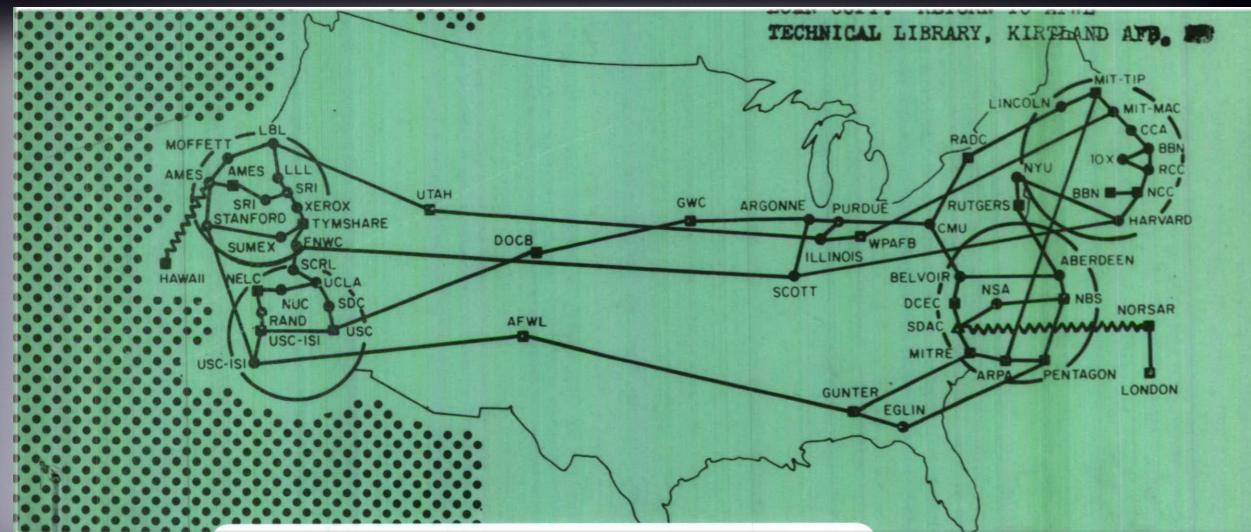
Infrastruttura di comunicazione



- Oggi tutti riconoscono questa immagine (hint)
- Nel '69 era un progetto che disegnava una infrastruttura di comunicazione - e diede le basi per la rete di comunicazione globale ;



Infrastruttura di comunicazione

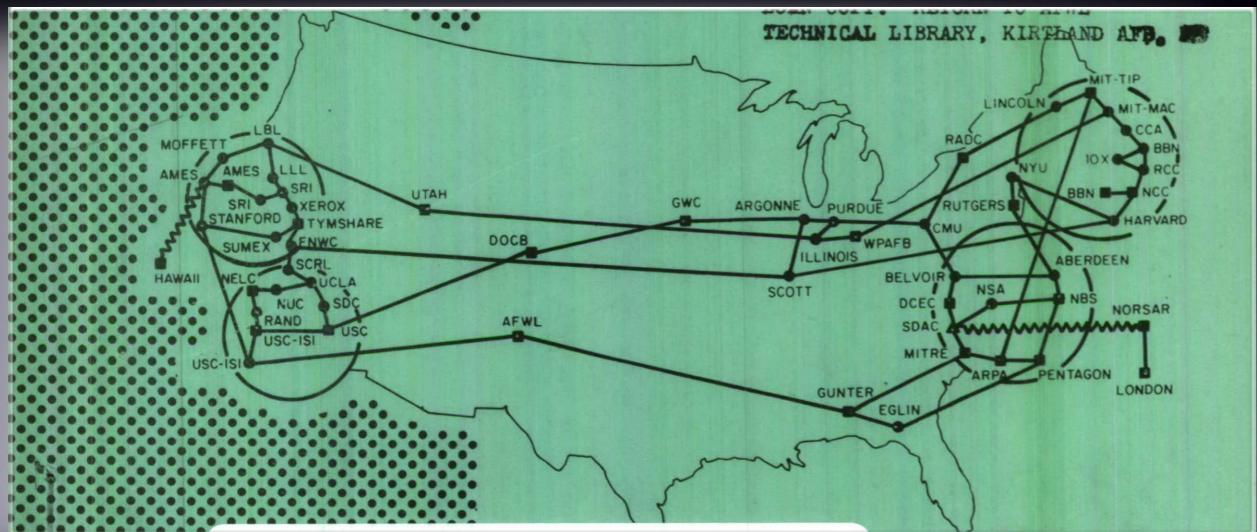


- Oggi tutti riconoscono questa immagine (hint)
- Nel '69 era un progetto che disegnava una infrastruttura di comunicazione - e diede le basi per la rete di comunicazione globale ;



Infrastruttura di comunicazione

- Oggi tutti riconoscono questa immagine (hint)

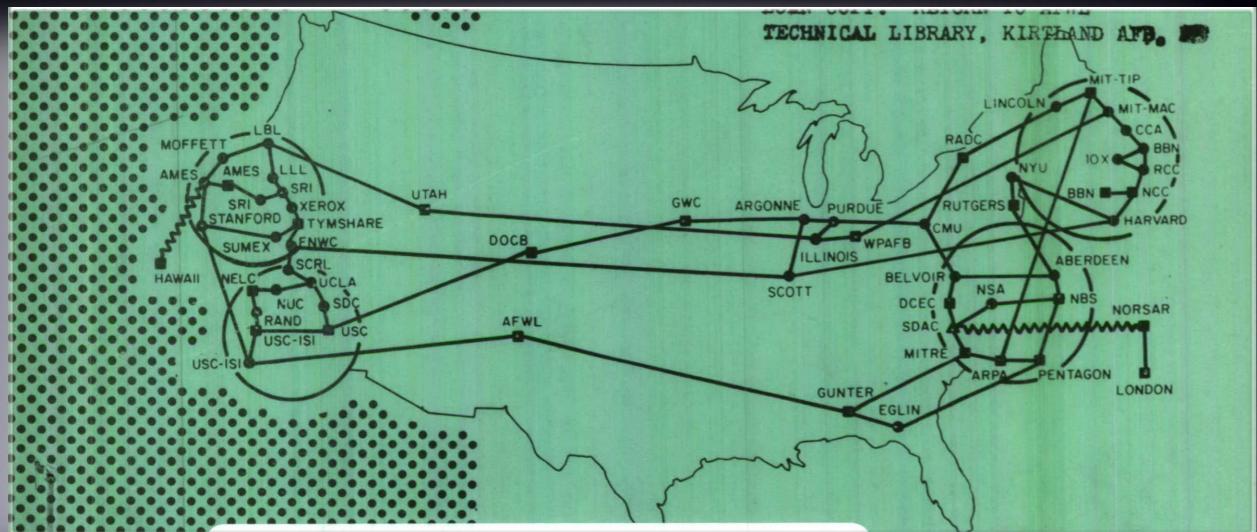


- Nel '69 era un progetto che disegnava una infrastruttura di comunicazione - e diede le basi per la rete di comunicazione globale ;
- Le caratteristiche studiate allora, ne hanno decretato la diffusione, **internet** è potuta diventare strumento di comunicazione globale grazie alle caratteristiche nel disegno iniziale.



Infrastruttura di comunicazione

- Oggi tutti riconoscono questa immagine (hint)



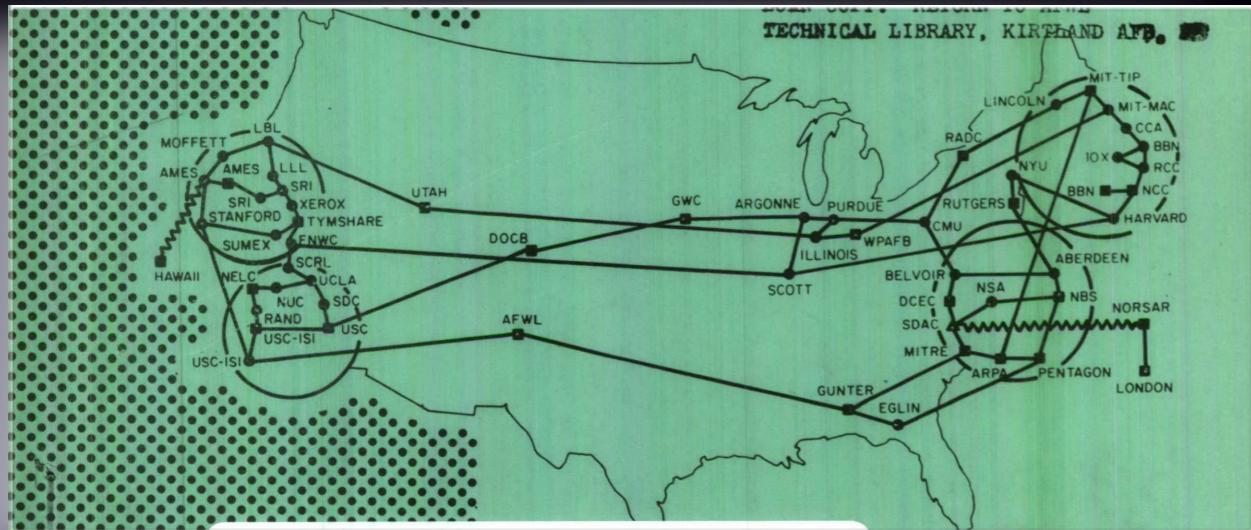
Aperta

- Nel '69 era un progetto che disegnava una infrastruttura di comunicazione - e diede le basi per la rete di comunicazione globale ;
- Le caratteristiche studiate allora, ne hanno decretato la diffusione, **internet** è potuta diventare strumento di comunicazione globale grazie alle caratteristiche nel disegno iniziale.



Infrastruttura di comunicazione

- Oggi tutti riconoscono questa immagine (hint)



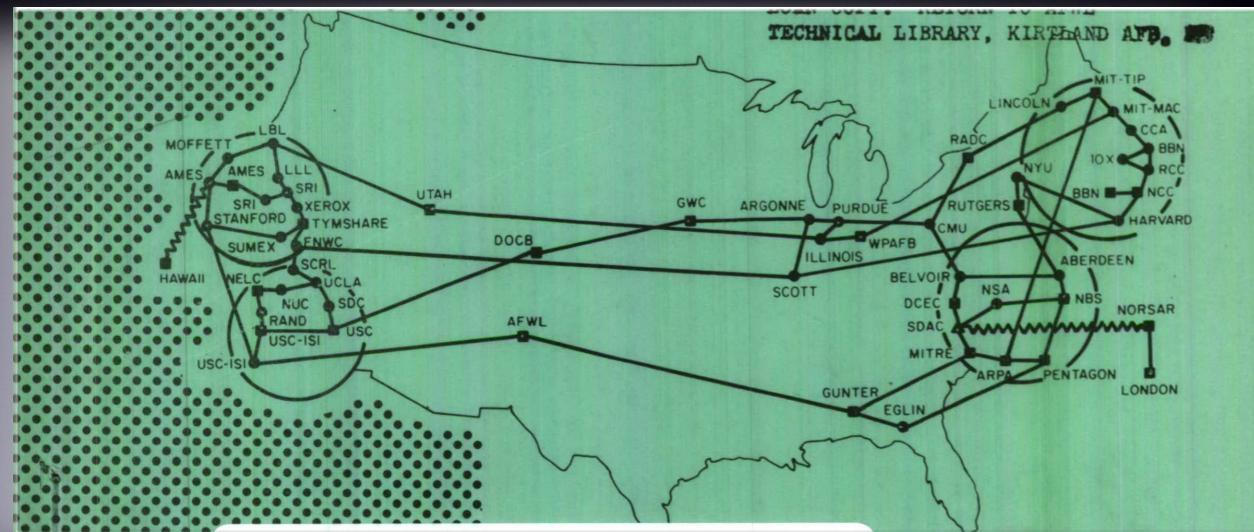
Aperta

Affidabile

- Nel '69 era un progetto che disegnava una infrastruttura di comunicazione - e diede le basi per la rete di comunicazione globale ;
- Le caratteristiche studiate allora, ne hanno decretato la diffusione, **internet** è potuta diventare strumento di comunicazione globale grazie alle caratteristiche nel disegno iniziale.



Infrastruttura di comunicazione



Aperta

Affidabile

Distribuita

- Oggi tutti riconoscono questa immagine (hint)
- Nel '69 era un progetto che disegnava una infrastruttura di comunicazione - e diede le basi per la rete di comunicazione globale ;
- Le caratteristiche studiate allora, ne hanno decretato la diffusione, **internet** è potuta diventare strumento di comunicazione globale grazie alle caratteristiche nel disegno iniziale.



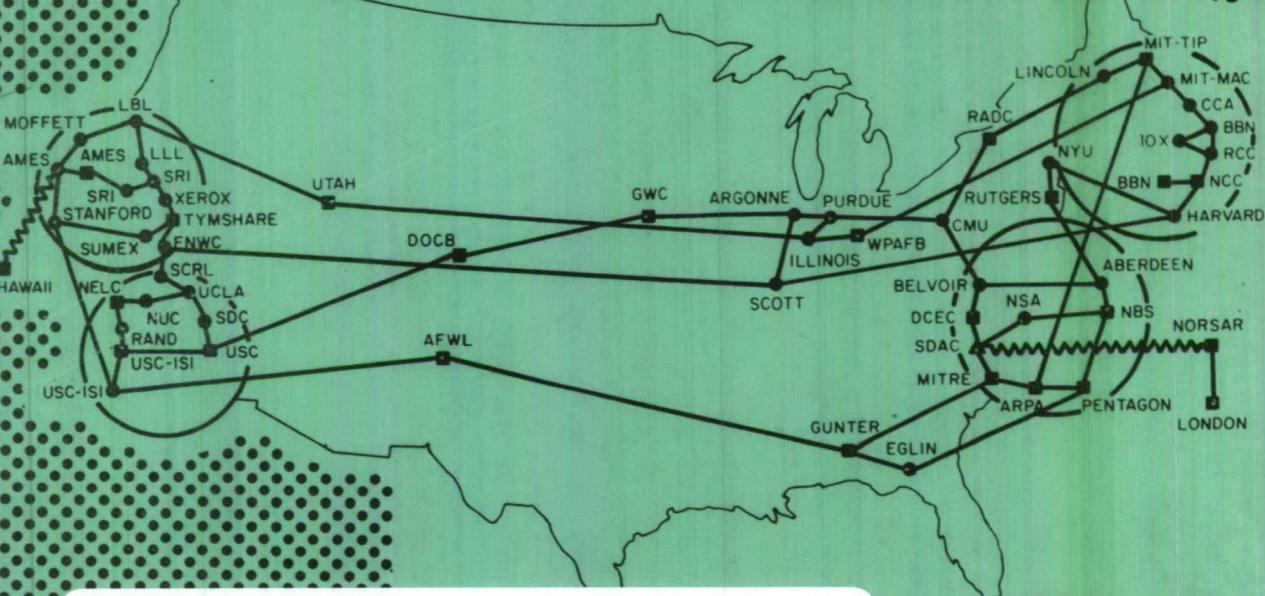
DCA
Z001
c.2



DDC
REF ID:
APR 14 1978
B

ARPANET INFORMATION BROCHURE

LOAN COPY: RETURN TO AFWL
TECHNICAL LIBRARY, KIRTLAND AFB.



20080514410

DEFENSE
COMMUNICATIONS
AGENCY

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

Il disegno
riflesso nel lato
applicativo

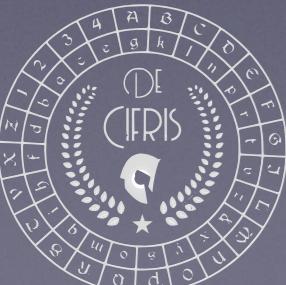
internet



Il disegno riflesso nel lato applicativo

dopo 50 anni, le applicazioni che pretendiamo di utilizzare in rete, declinano nel proprio ambito quegli stessi principi

internet



Il disegno riflesso nel lato applicativo

dopo 50 anni, le applicazioni che pretendiamo di utilizzare in rete, declinano nel proprio ambito quegli stessi principi

le applicazioni crittografiche
non fanno eccezione

internet



Il disegno riflesso nel lato applicativo

dopo 50 anni, le applicazioni che pretendiamo di utilizzare in rete, declinano nel proprio ambito quegli stessi principi

le applicazioni crittografiche
non fanno eccezione

internet

?



Il disegno riflesso nel lato applicativo

dopo 50 anni, le applicazioni che pretendiamo di utilizzare in rete, declinano nel proprio ambito quegli stessi principi

le applicazioni crittografiche
non fanno eccezione

Affidabile

internet

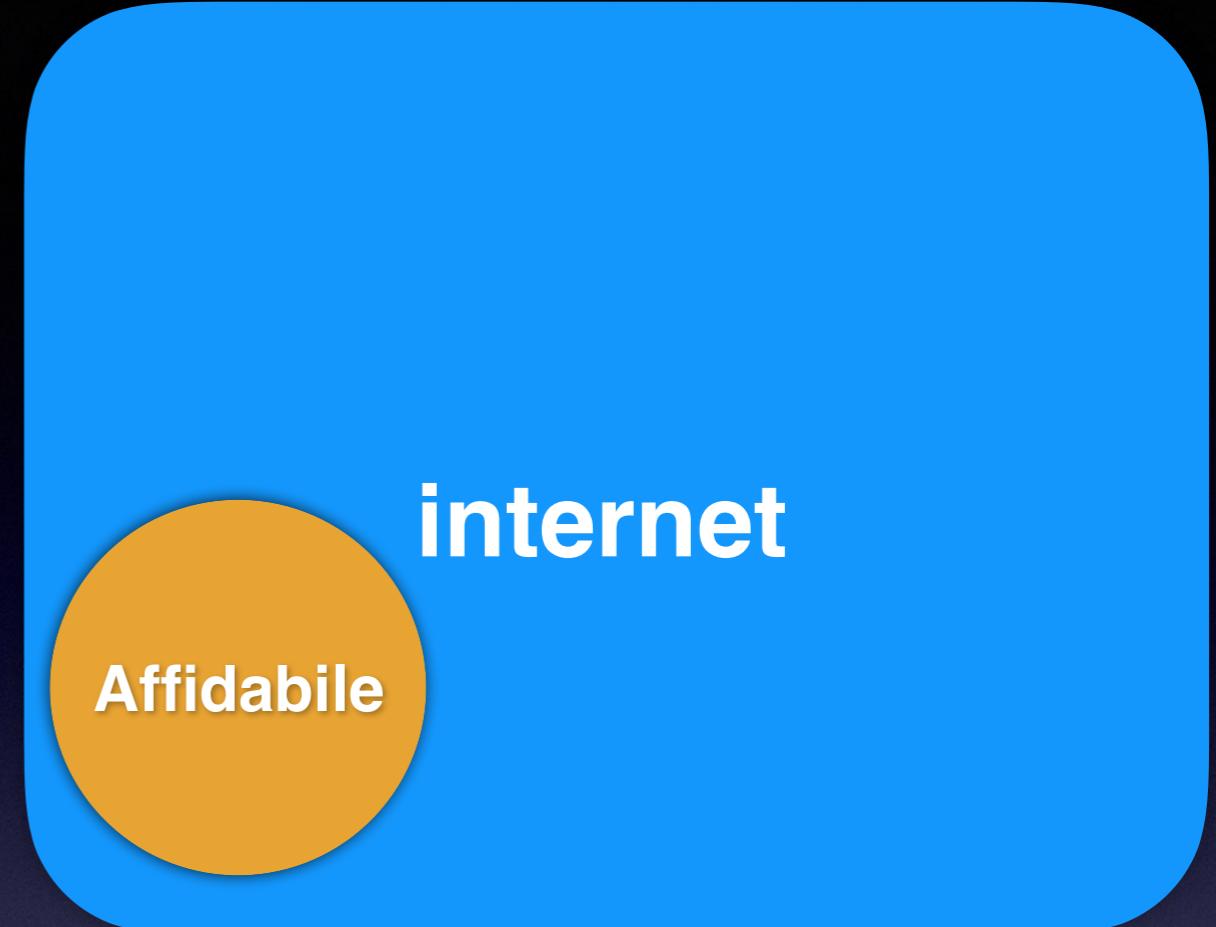
?



Il disegno riflesso nel lato applicativo

dopo 50 anni, le applicazioni che pretendiamo di utilizzare in rete, declinano nel proprio ambito quegli stessi principi

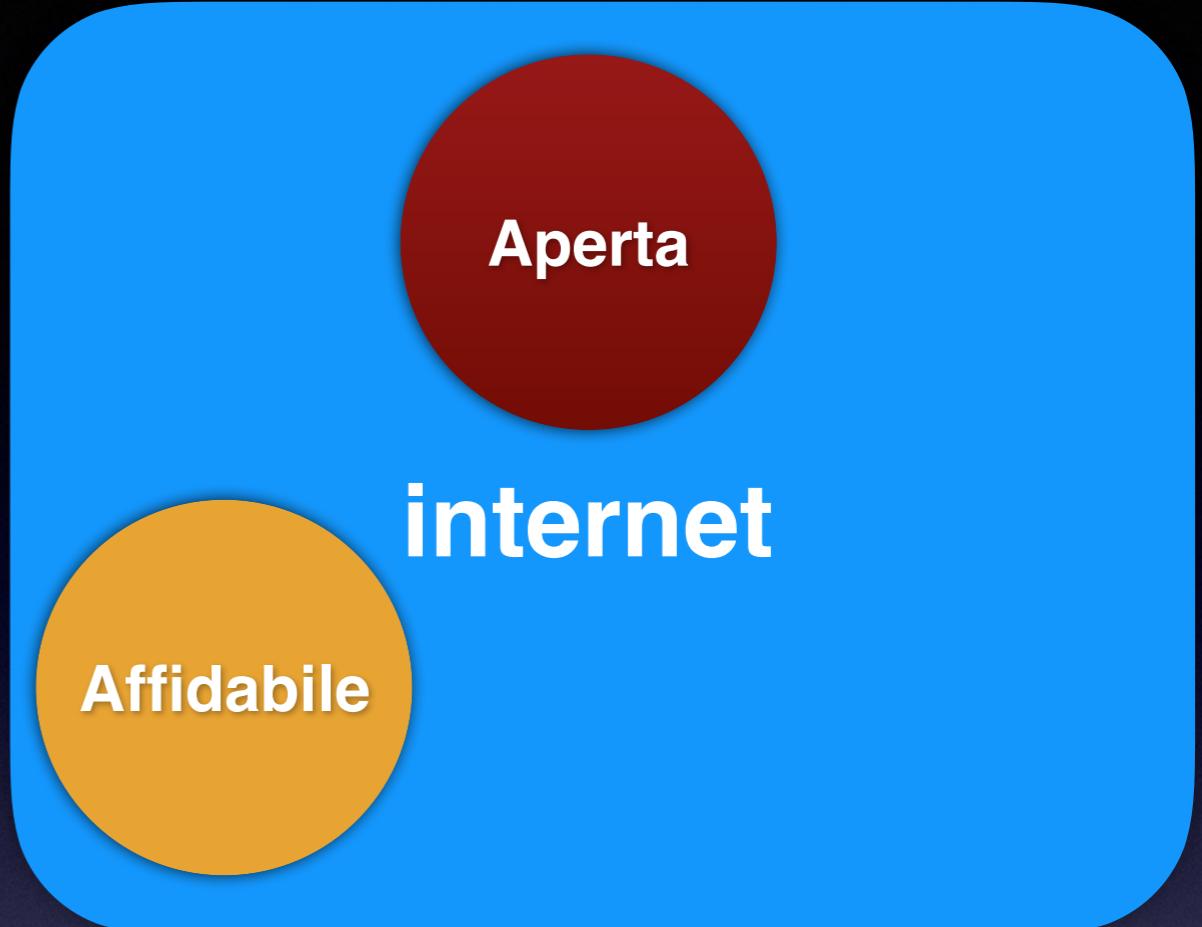
le applicazioni crittografiche
non fanno eccezione



Il disegno riflesso nel lato applicativo

dopo 50 anni, le applicazioni che pretendiamo di utilizzare in rete, declinano nel proprio ambito quegli stessi principi

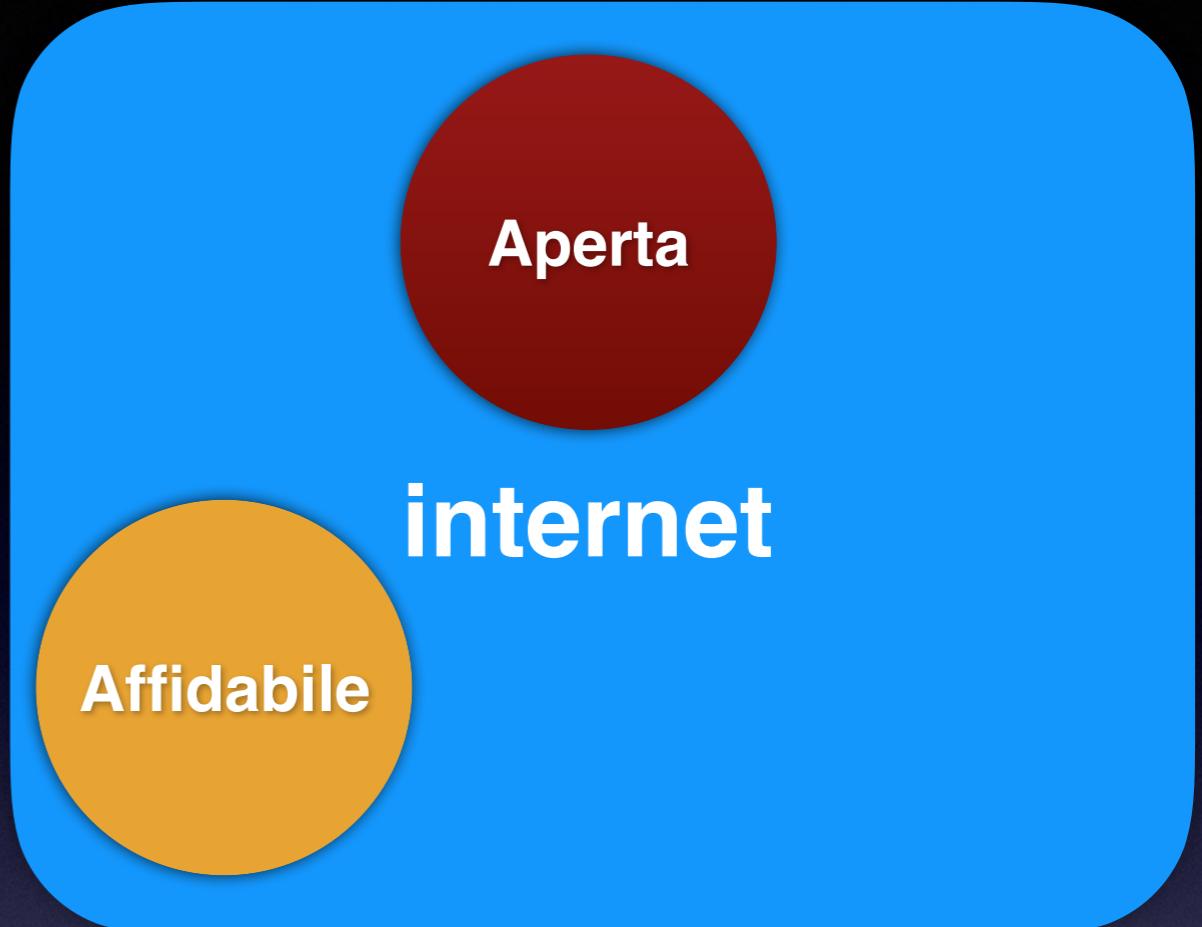
le applicazioni crittografiche
non fanno eccezione



Il disegno riflesso nel lato applicativo

dopo 50 anni, le applicazioni che pretendiamo di utilizzare in rete, declinano nel proprio ambito quegli stessi principi

le applicazioni crittografiche non fanno eccezione



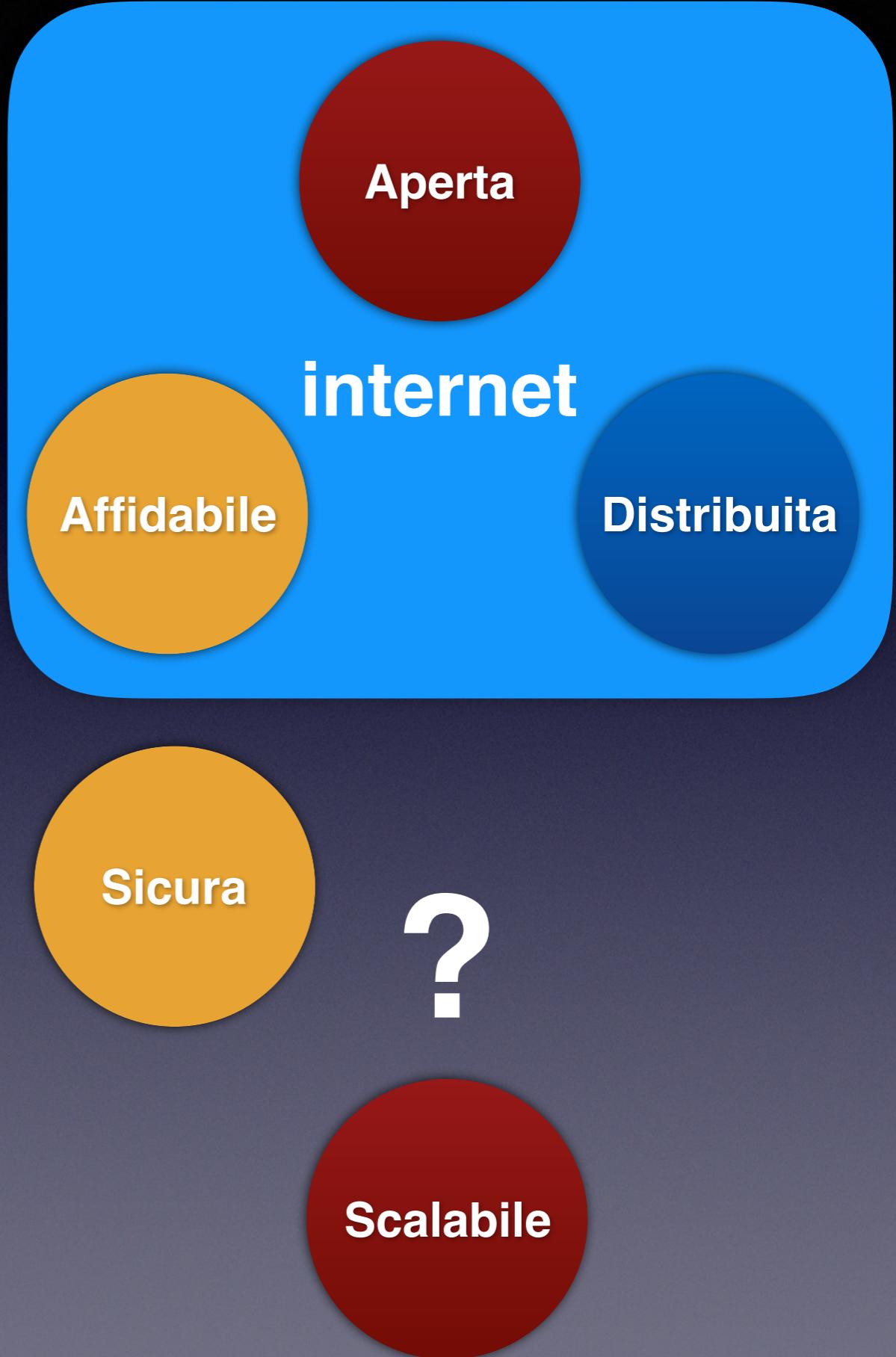
Scalabile



Il disegno riflesso nel lato applicativo

dopo 50 anni, le applicazioni che pretendiamo di utilizzare in rete, declinano nel proprio ambito quegli stessi principi

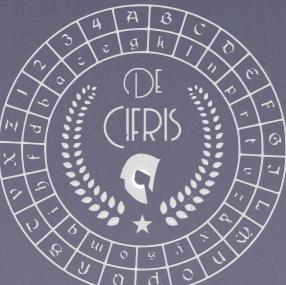
le applicazioni crittografiche
non fanno eccezione



Il disegno riflesso nel lato applicativo

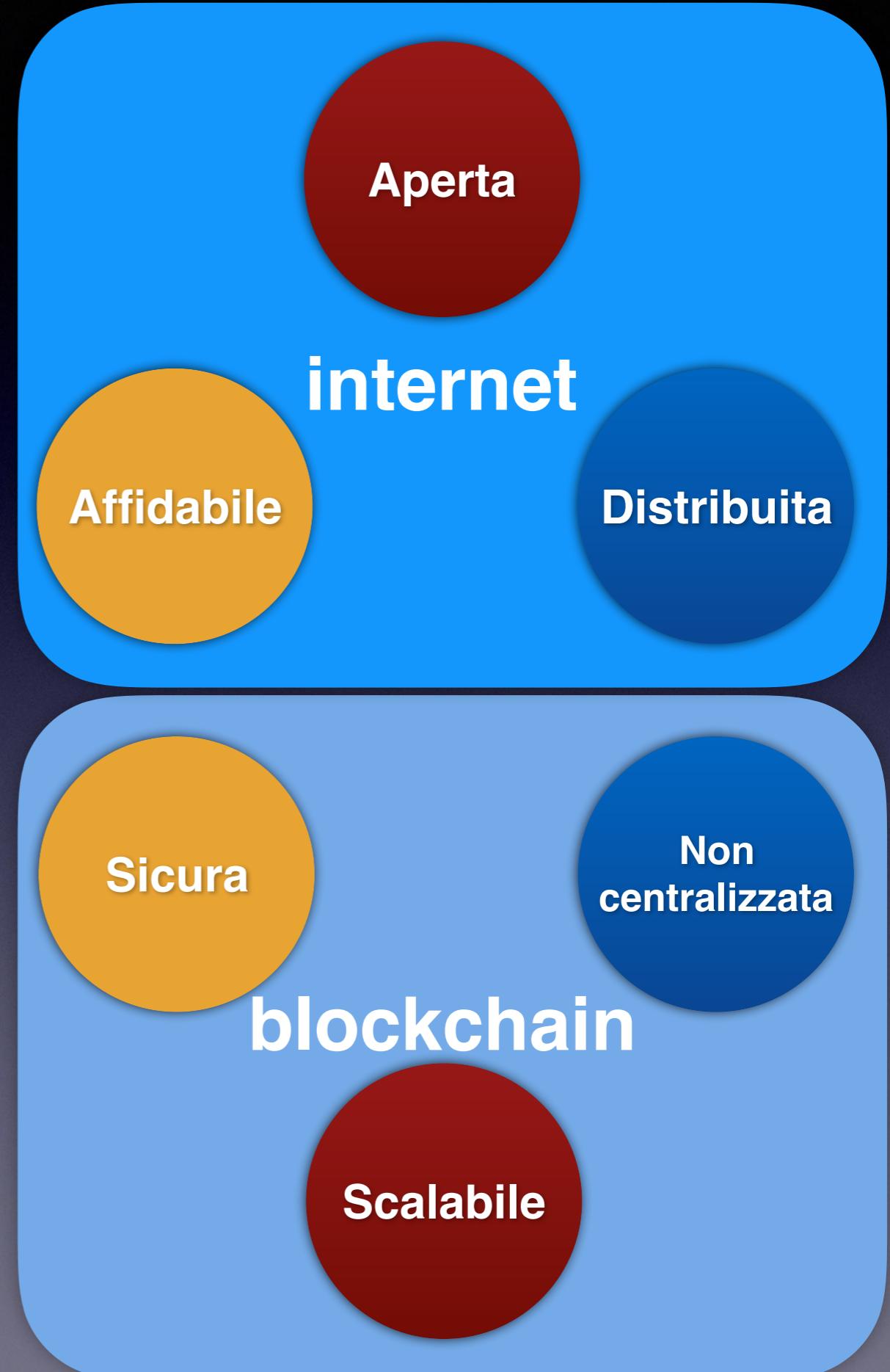
dopo 50 anni, le applicazioni che pretendiamo di utilizzare in rete, declinano nel proprio ambito quegli stessi principi

le applicazioni crittografiche non fanno eccezione



Il disegno riflesso nel lato applicativo

dopo 50 anni le applicazioni crittografiche (e non solo) di oggi sono costruite su una versione aggiornata di quelle caratteristiche



due facce
della stessa
medaglia

Affidabile

Sicura

Aperta

internet

Distribuita

Non
centralizzata

blockchain

Scalabile



due facce
della stessa
medaglia

Affidabile

Sicura

Aperta

in
**COMMUNICATIONS
AND
CRYPTOGRAPHY**

Two Sides of One Tapestry

edited by

Richard E. Blahut
Daniel J. Costello, Jr.
Ueli Maurer
Thomas Mittelholzer

blockchain

Scalabile



due facce della stessa medaglia

C. Shannon (1948) scrisse due lavori che hanno segnato l'inizio della **Teoria dell'Informazione** e della **Crittografia** nella loro versione moderna

Affidabile

Sicura

Aperta

COMMUNICATIONS
AND
CRYPTOGRAPHY

Two Sides of One Tapestry

edited by

Richard E. Blahut
Daniel J. Costello, Jr.
Ueli Maurer
Thomas Mittelholzer

blockchain

Scalabile



due facce della stessa medaglia

C. Shannon (1948) scrisse due lavori che hanno segnato l'inizio della **Teoria dell'Informazione** e della **Crittografia** nella loro versione moderna

Avere la **Ancita** sugli errori di comunicazione

Affidabile

Sicura

Scalabile

COMMUNICATIONS
AND
CRYPTOGRAPHY
Two Sides of One Tapestry

edited by

Richard E. Blahut
Daniel J. Costello, Jr.
Ueli Maurer
Thomas Mittelholzer

blockchain



due facce della stessa medaglia

C. Shannon (1948) scrisse due lavori che hanno segnato l'inizio della **Teoria dell'Informazione** e della **Crittografia** nella loro versione moderna

Avere la **Ancita** sugli errori di comunicazione

Affidabile

Sicura

**COMMUNICATIONS
AND
CRYPTOGRAPHY**
Two Sides of One Tapestry

edited by

Richard E. Blahut
Daniel J. Costello, Jr.
Ueli Maurer
Thomas Mittelholzer

blockchain

Aggiungere abbastanza errori da rendere impossibile l'intercettazione

Scalabile



Punto-punto

La Teoria di Shannon definisce le proprietà della comunicazione tra due entità - così come la struttura di base per internet è la connessione punto-punto.

Affidabile

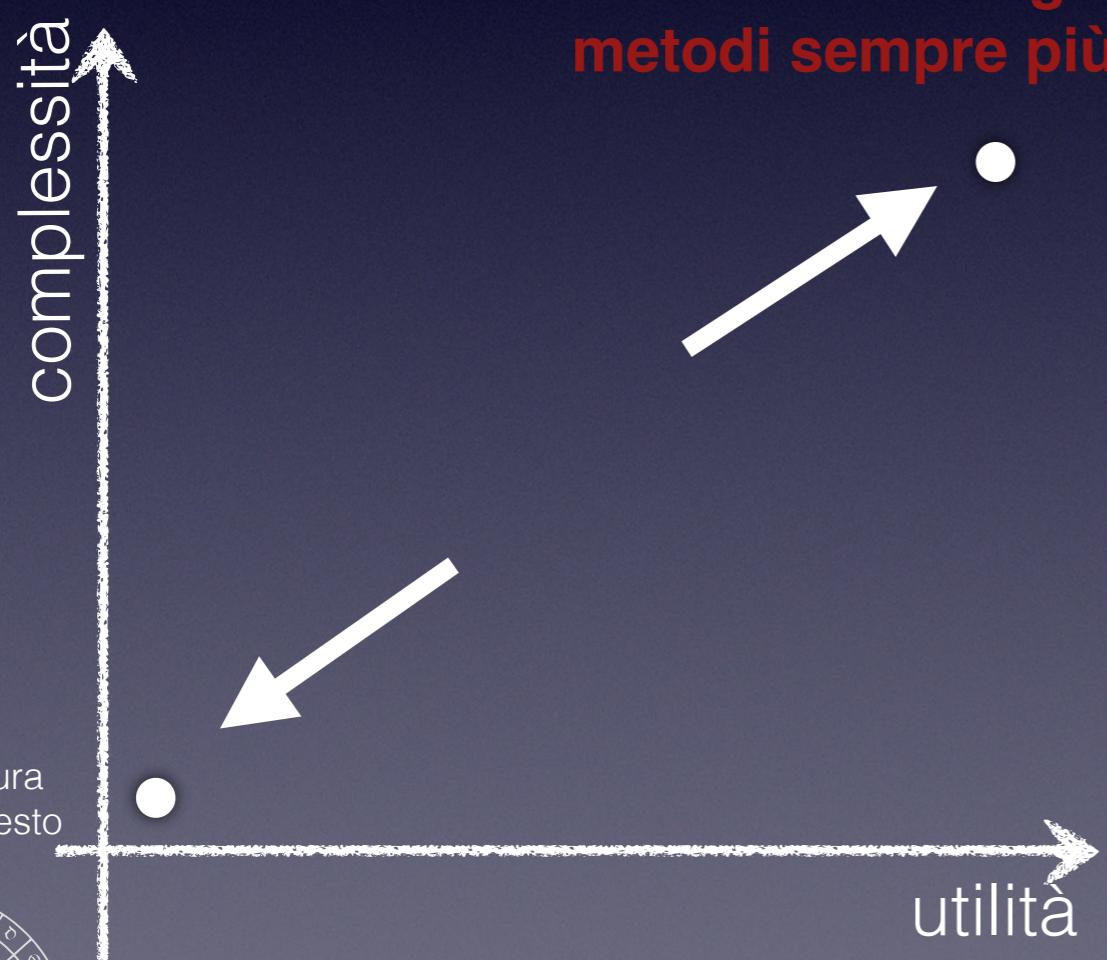
Sicura



- La **matematica** in azione nelle due versioni è molto simile
- E' stata sviluppata e declinata in molteplici forme e ci fornisce una serie di strumenti per risolvere i problemi di comunicazione
- L'ambito di applicazione si è esteso (grazie al disegno originale) e la **complessità** dei problemi di comunicazione è aumentata

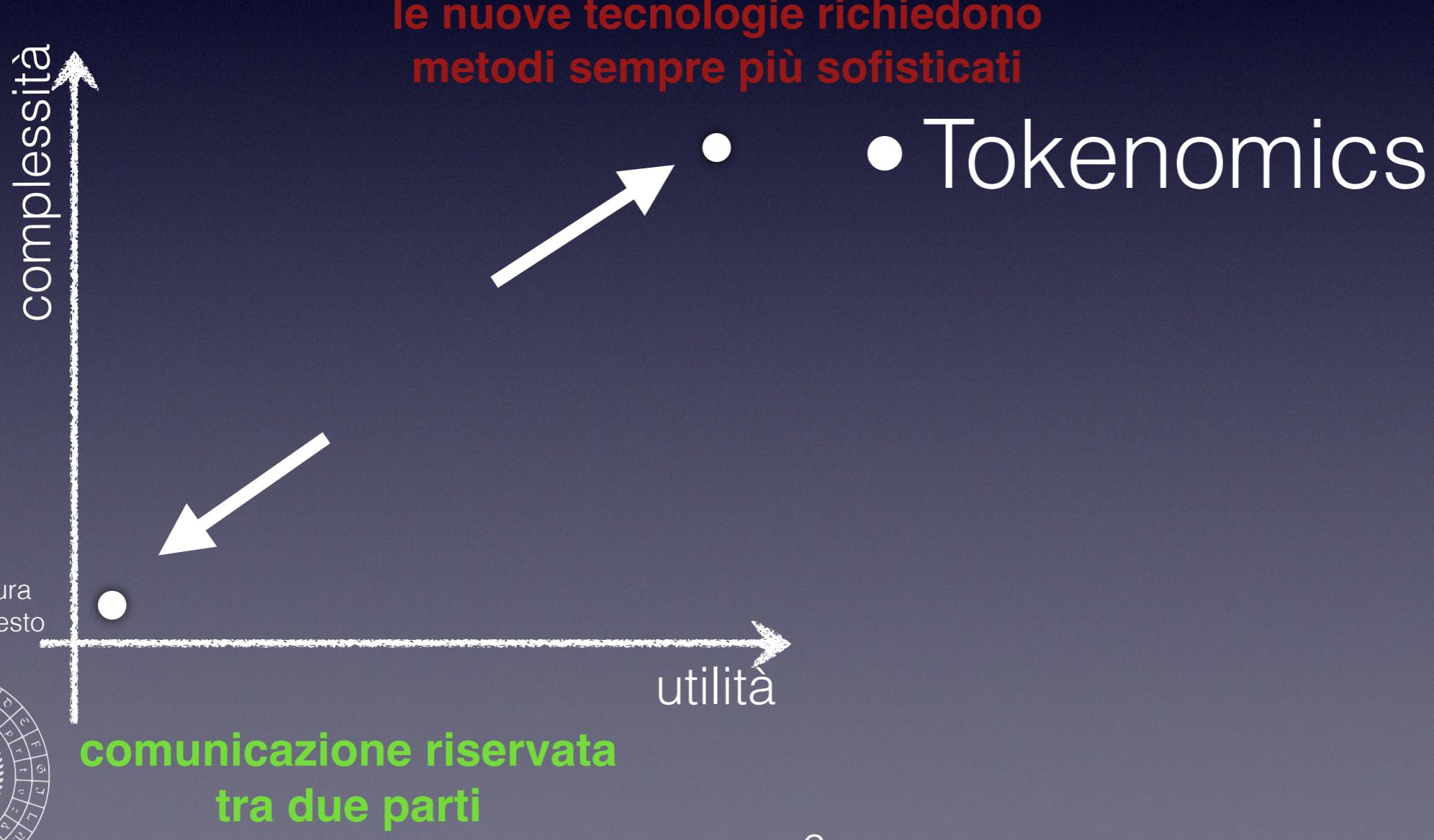
Complessità vs Utilità

la tensione tra l'**aumento di complessità** richiesto alla crittografia e l'evoluzione dell'esigenza di **utilizzo in nuove situazioni**



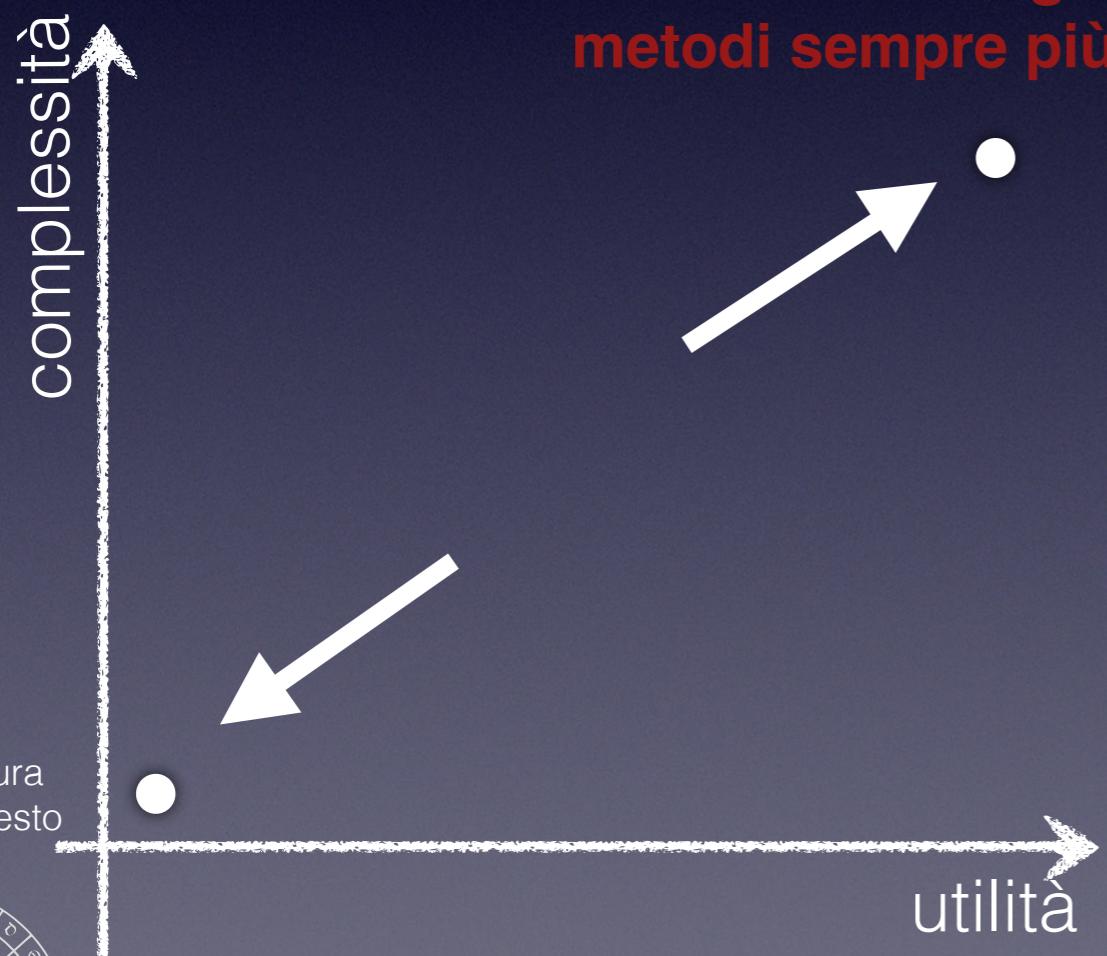
Complessità vs Utilità

la tensione tra l'**aumento di complessità** richiesto alla crittografia e l'evoluzione dell'esigenza di **utilizzo in nuove situazioni**



Complessità vs Utilità

la tensione tra l'**aumento di complessità** richiesto alla crittografia e l'evoluzione dell'esigenza di **utilizzo in nuove situazioni**



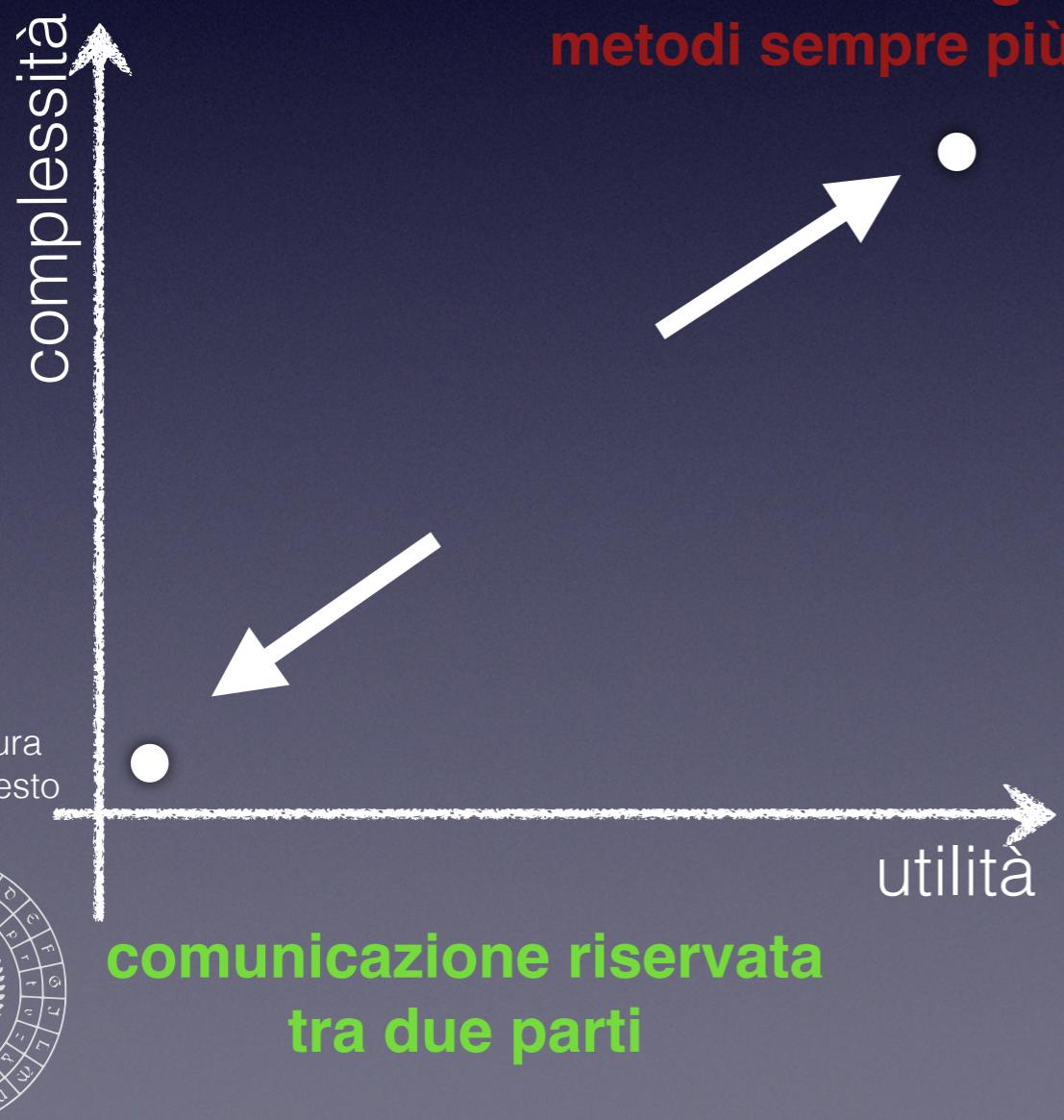
- Tokenomics
- Biometria

comunicazione riservata
tra due parti



Complessità vs Utilità

la tensione tra l'**aumento di complessità** richiesto alla crittografia e l'evoluzione dell'esigenza di **utilizzo in nuove situazioni**



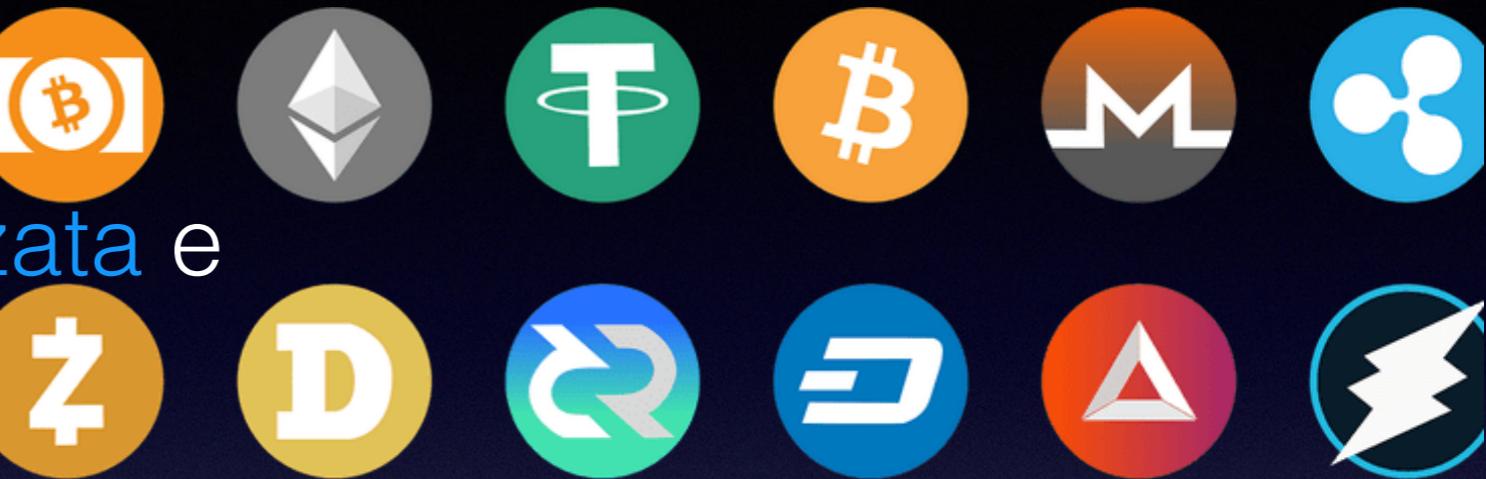
le nuove tecnologie richiedono
metodi sempre più sofisticati

- Tokenomics
- Biometria
- Cloud Computing

Esempi di Attuazione

- **Tokenomics:**

- infrastruttura per gli **scambi** economici
- architettura software: **sicura, non-centralizzata e scalabile**



- **Biometric Data**

- key extraction
- **identity** based authentication
- privacy



- **Federated Computation**

- **condivisione** di risorse
- garanzie in caso di conferimenti a terze parti



crittotecnologie



crittoteconomie crittografia



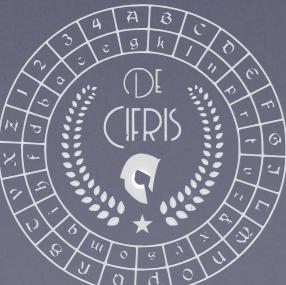
crittoteconomie crittografia

- Crittografia a chiave pubblica
- Funzioni di Hash
- Codici non malleabili
- Fuzzy Encryption
- Differential Privacy
- Learning with Errors
- Garbled Circuits
- Lattice Encryption
- Interactive Protocols



crittoteconomie crittografia

- **Tokenomics**
 - Blockchain
 - Cryptocurrency
 - Smart Contracts
- Crittografia a chiave pubblica
- Funzioni di Hash
- Codici non malleabili
- Fuzzy Encryption
- Differential Privacy
- Learning with Errors
- Garbled Circuits
- Lattice Encryption
- Interactive Protocols



crittoteconomie crittografia

- **Tokenomics**
 - Blockchain
 - Cryptocurrency
 - Smart Contracts
- **Biometric Data**
 - Identity Based Encryption
 - Key Extraction
 - Identity Protection
- Crittografia a chiave pubblica
- Funzioni di Hash
- Codici non malleabili
- Fuzzy Encryption
- Differential Privacy
- Learning with Errors
- Garbled Circuits
- Lattice Encryption
- Interactive Protocols



crittoteconomie crittografia

- **Tokenomics**
 - Blockchain
 - Cryptocurrency
 - Smart Contracts
- **Biometric Data**
 - Identity Based Encryption
 - Key Extraction
 - Identity Protection
- **Federated Computation**
 - Zero Knowledge
 - Multiparty computation
- Crittografia a chiave pubblica
- Funzioni di Hash
- Codici non malleabili
- Fuzzy Encryption
- Differential Privacy
- Learning with Errors
- Garbled Circuits
- Lattice Encryption
- Interactive Protocols

Crittografia Omomorfa



alcune crittotecnologie attualmente
nate dalla combinazione di
metodi della crittografia

Blockchain

Funzioni di hash

Cifratura a chiave pubblica

Crittografia

Registro immutabile
e verificabile di transazioni

Crittoteconomia

implementazione di una
infrastruttura software
con uno scopo applicativo



Blockchain

Funzioni di hash

Cifratura a chiave pubblica

Crittografia

Registro immutabile
e verificabile di transazioni

Crittoteconomia

implementazione di una
infrastruttura software
con uno scopo applicativo

EVM (ethereum
virtual machine)



Key Extraction

Identity Based Encryption:

- inventata da Shamir (1984)
- schema di cifratura a chiave pubblica senza bisogno di predistribuire le chiavi pubbliche
- basata su un servizio affidabile (trusted server) per la distribuzione delle chiavi.

Biometria:

- lettura dell'**iride**
- rilevatori di parametri fisiologici (**EEG**, **ECG**)

la chiave estratta dai parametri biometrici sarà sempre affetta da rumore per questo è necessario sviluppare funzioni di cifratura che tollerano imprecisioni.



Fuzzy Encryption

Dodis-Reyzin-Smith (Eurocrypt 2004) definiscono:

- una tecnica efficiente e sicura per convertire le informazioni biometriche in chiavi crittografiche
- autenticare in modo affidabile e sicuro tramite i dati biometrici

Realizzano un **fuzzy extractor** in grado di costruire in modo **robusto** una sequenza casuale a partire dal dato biometrico, nel senso che un dato biometrico leggermente diverso produce la stessa sequenza randomica.

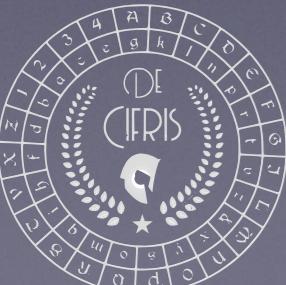


Multiparty Computation

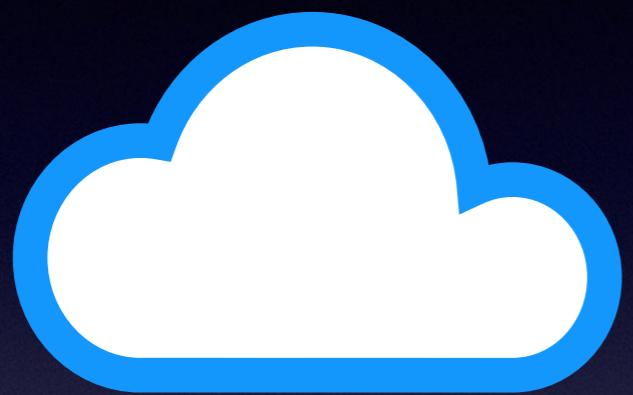
- Definire una **funzione di cifratura** il cui valore può essere calcolato solo coinvolgendo tutti o almeno una frazione fissata di partecipanti
- La crittografia in azione è realizzata mediante:
 - **secret sharing** (condivisione di segreto)
 - esempio: Shamir (1979) utilizzando l'interpolazione di Lagrange si può calcolare il valore di un certo polinomio (di grado t) se ci sono t contributi corretti su n partecipanti.
 - **oblivious transfer** (trasferimento immemore)
 - esempio: Rabin (1981) trasferire un'informazione con una certa probabilità senza sapere se il trasferimento è avvenuto
 - **commitment scheme** (schema di impegno)
 - esempio: Blum (1982) *coin flipping by telephone*

Problema dei Milionari

- Uno dei primi esempi di MPC che è anche diventato un classico per spiegare MPC è la soluzione del PM di Yao (1982):
- due milionari vogliono stabilire chi dei due sia il più ricco senza rilevare all'altro l'entità del proprio patrimonio
- **Soluzione:** i protocolli per ***oblivious transfer*** e una versione efficiente utilizzando lo schema di cifratura di Goldwasser-Micali (1982) e più di recente utilizzando la cifratura omomorfa in Ling-Tzeng (2005).



Non Decifrare Mai !!



cloud

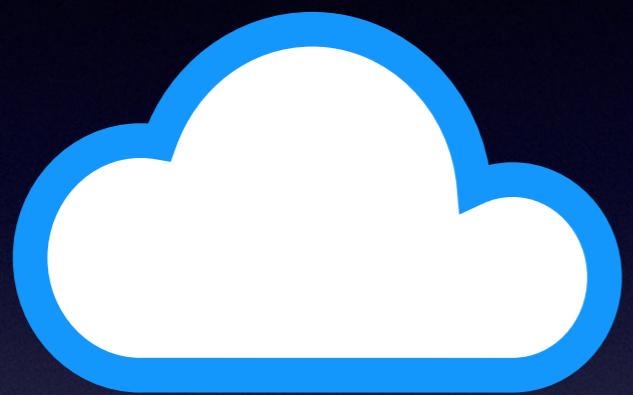


transport



user data

Non Decifrare Mai !!



cloud



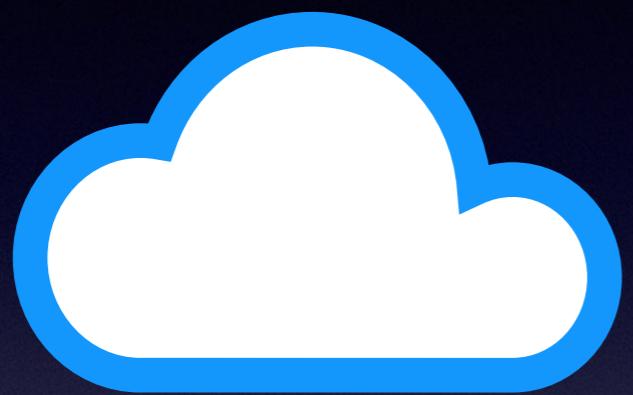
transport



user data

data

Non Decifrare Mai !!



cloud



transport

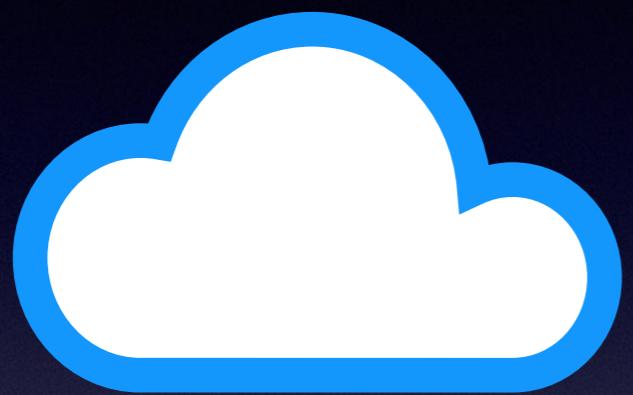


user data



data

Non Decifrare Mai !!



cloud



transport

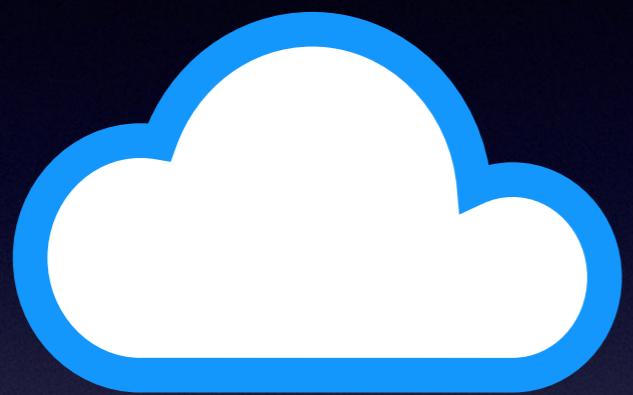


user data

data
↓

$x = \text{Enc}(\text{data}, \text{key})$

Non Decifrare Mai !!



cloud



transport



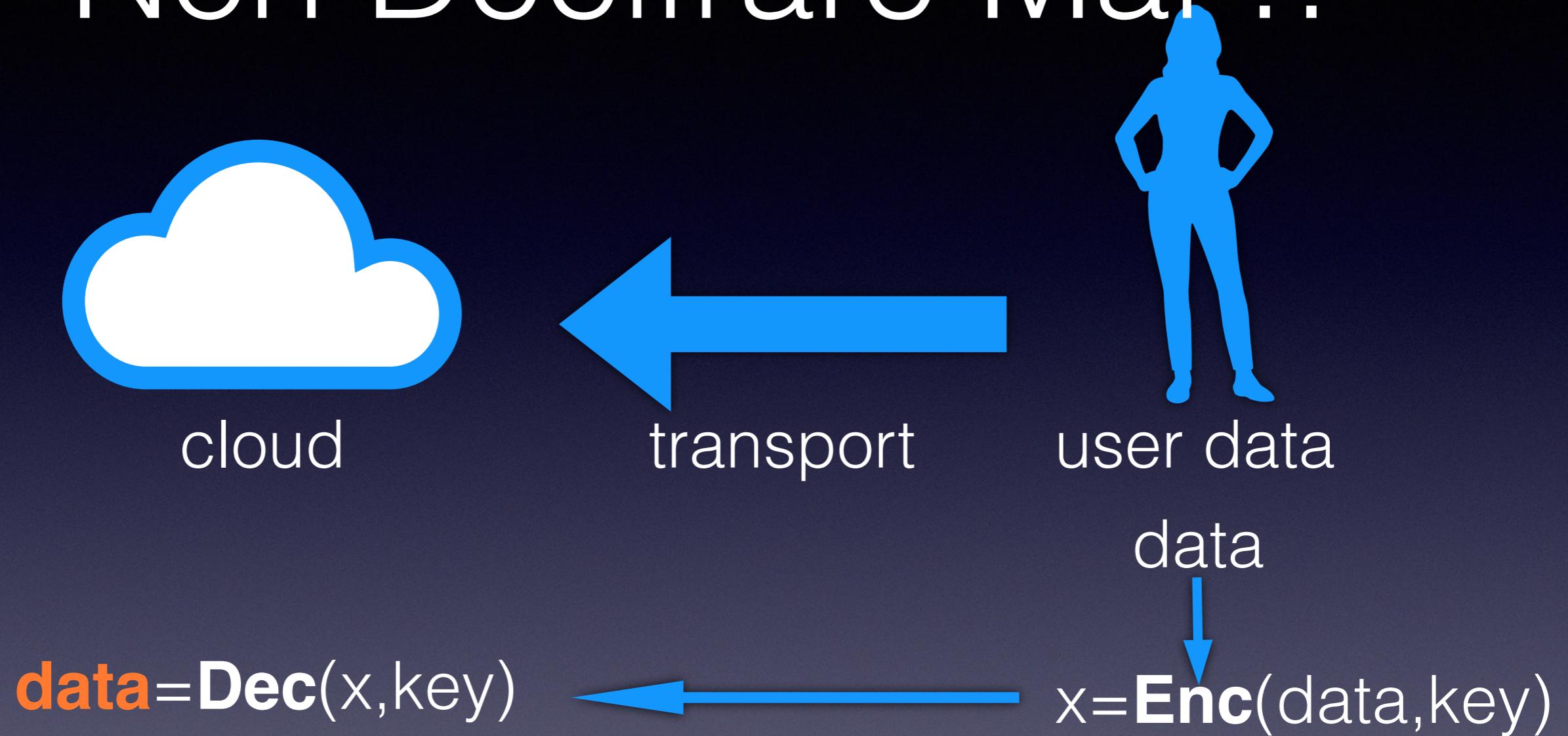
user data

data
↓

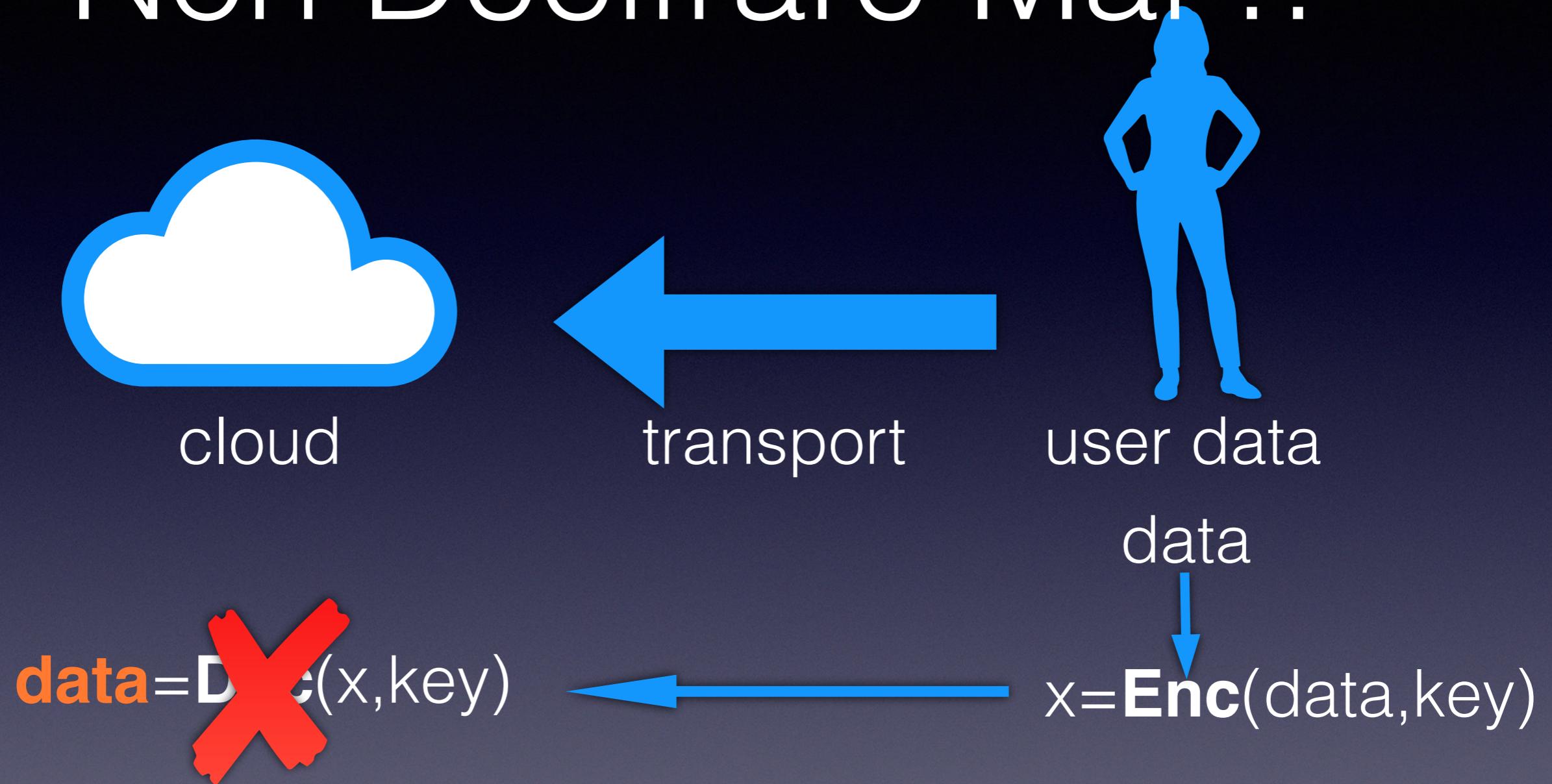


$x = \text{Enc}(\text{data}, \text{key})$

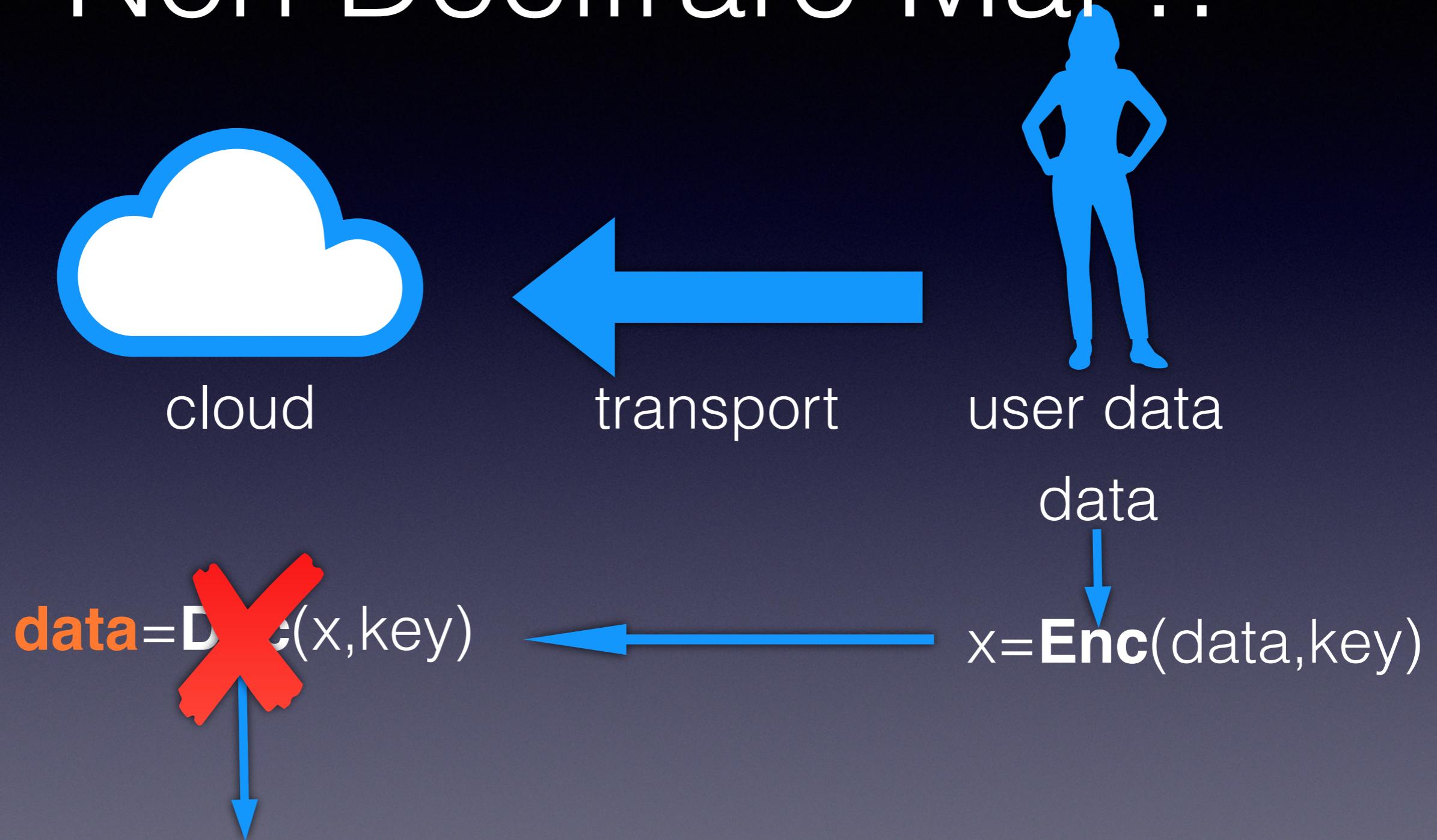
Non Decifrare Mai !!



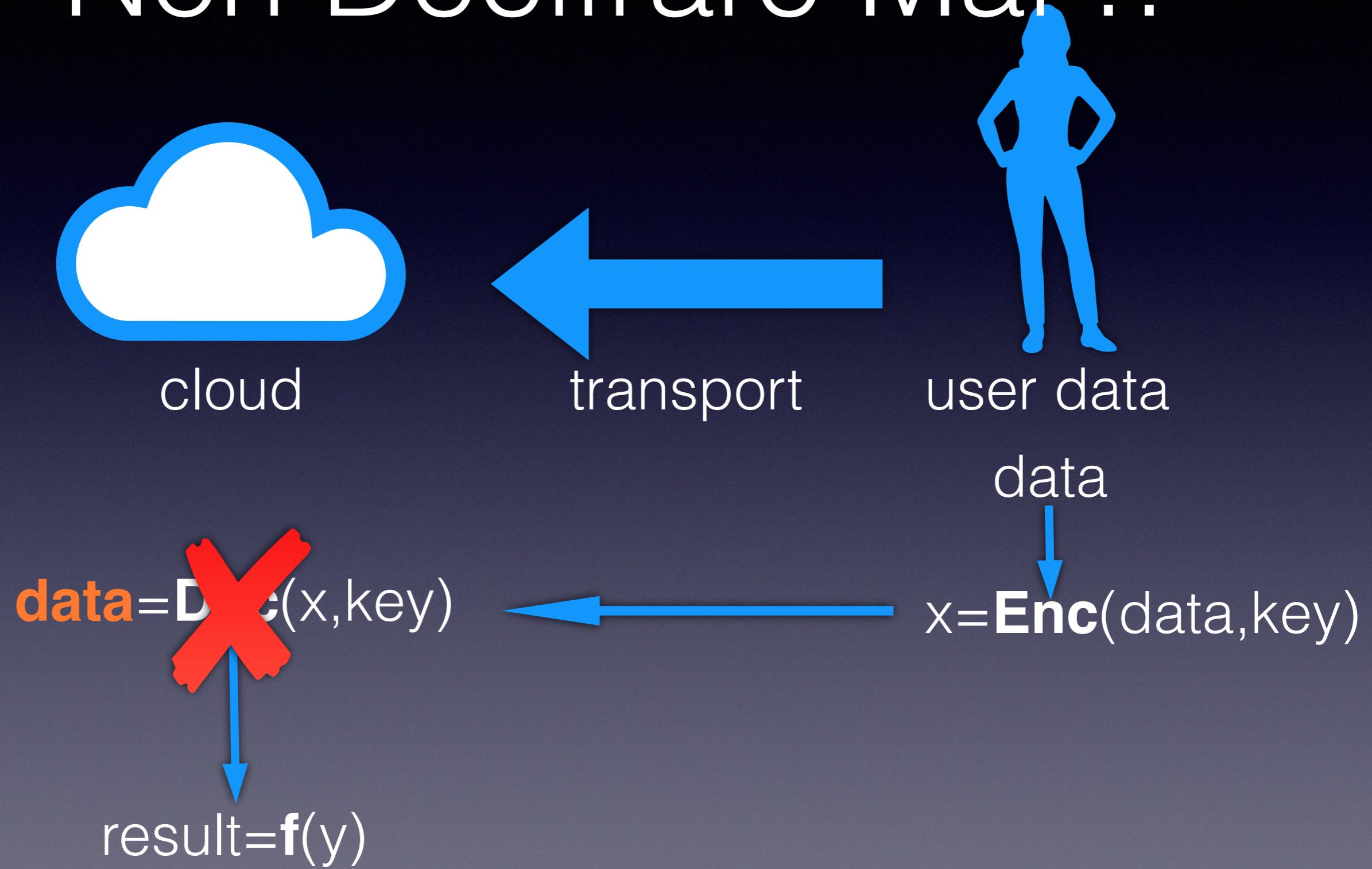
Non Decifrare Mai !!



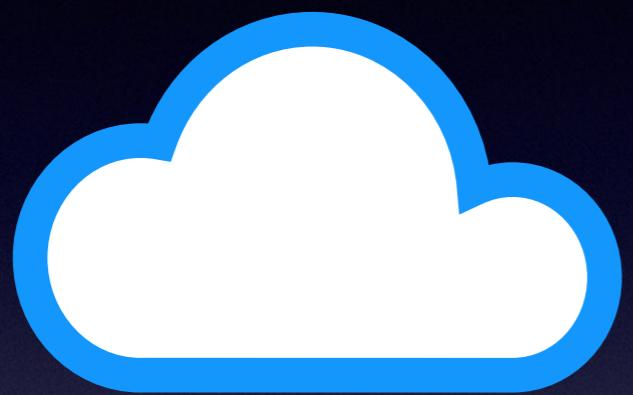
Non Decifrare Mai !!



Non Decifrare Mai !!



Homomorphic Encryption



cloud



transport



user data

Homomorphic Encryption



cloud



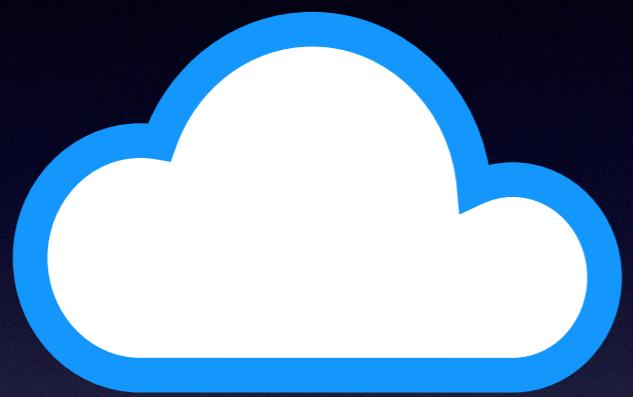
transport



user data

data

Homomorphic Encryption



cloud



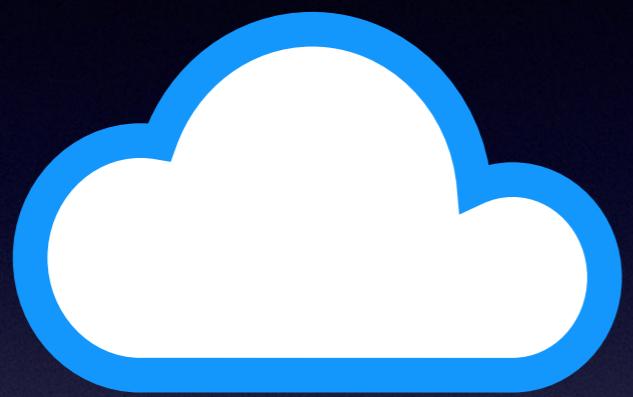
transport



user data

data
↓

Homomorphic Encryption



cloud



transport

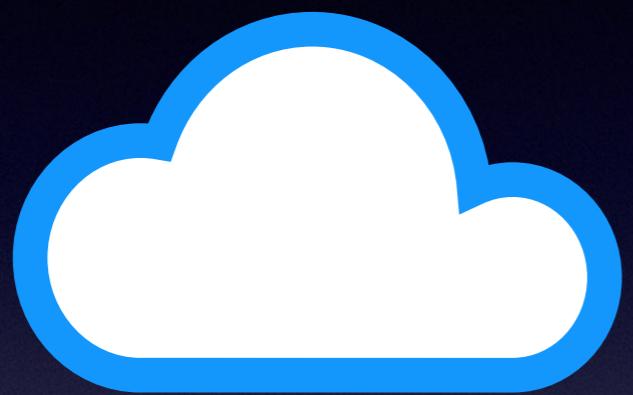


user data

data
↓

$x = \text{Enc}(\text{data}, \text{key})$

Homomorphic Encryption



cloud



transport



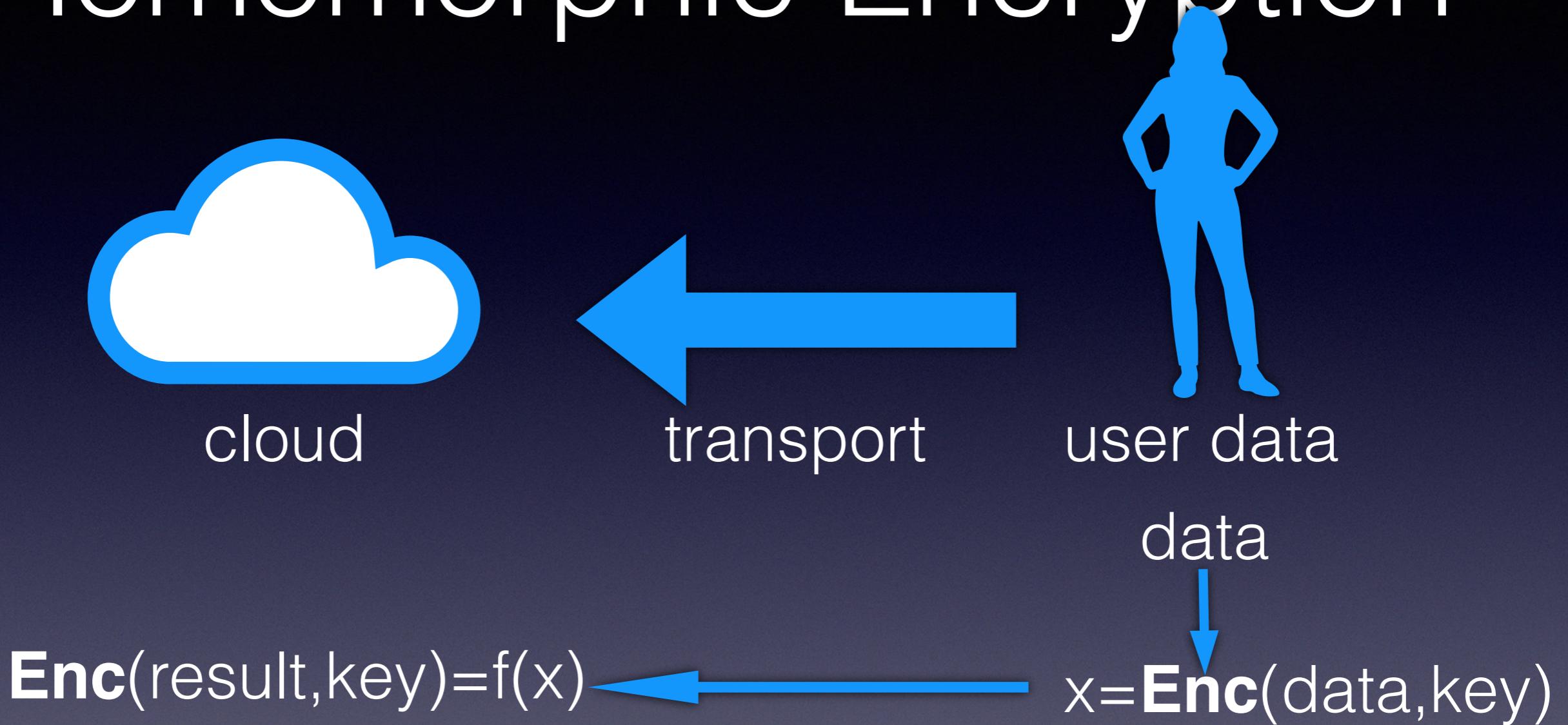
user data

data
↓

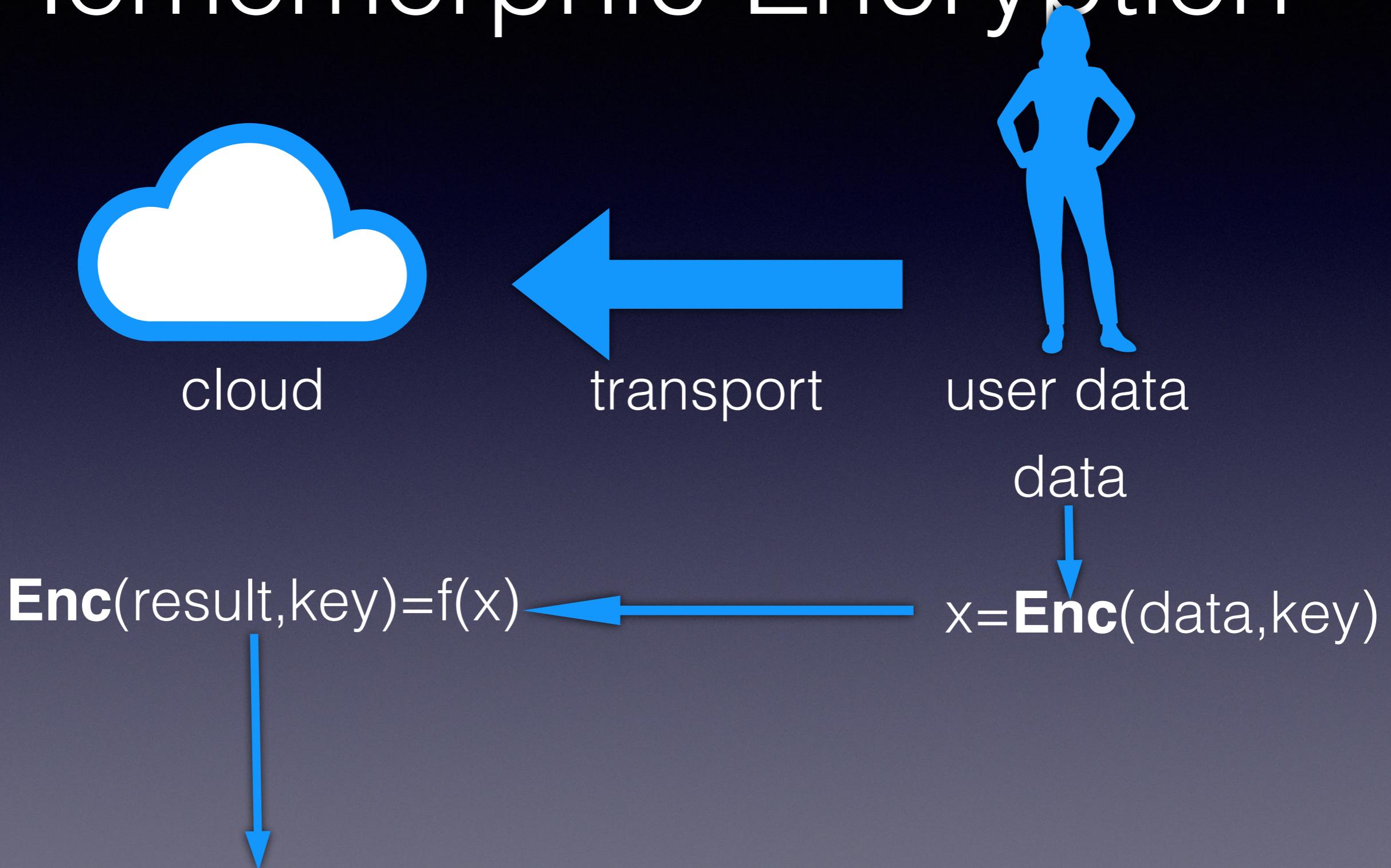


$x = \text{Enc}(\text{data}, \text{key})$

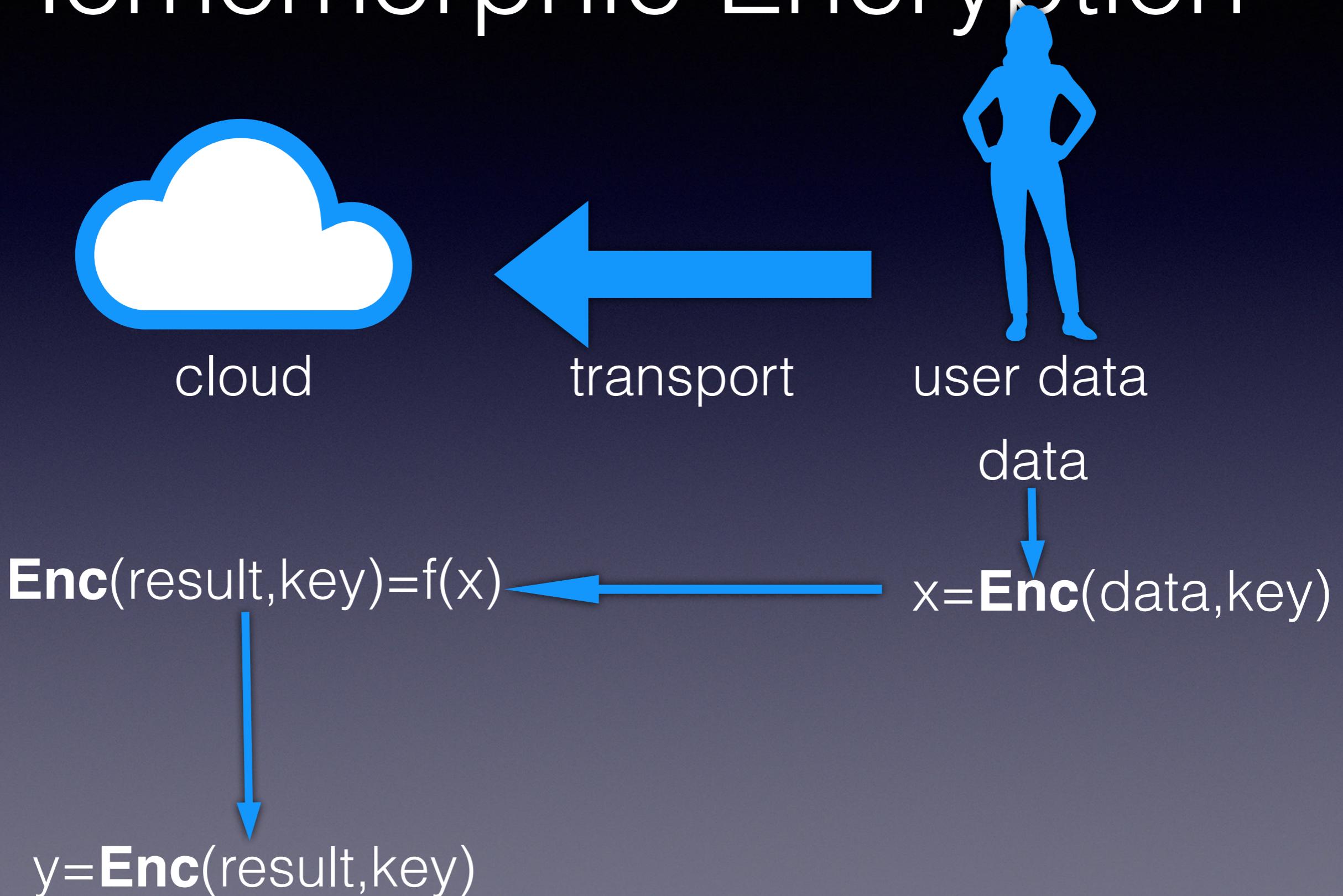
Homomorphic Encryption



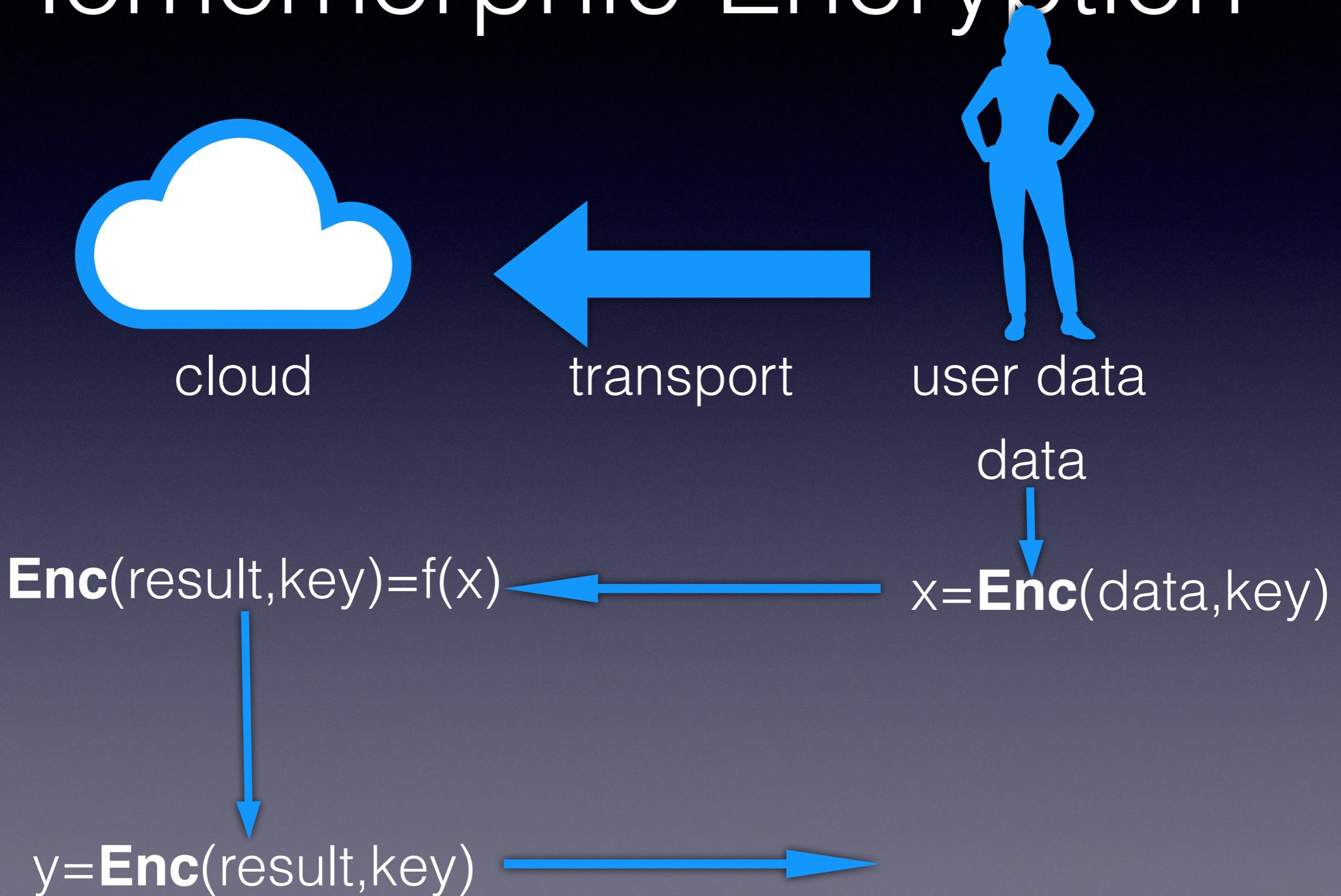
Homomorphic Encryption



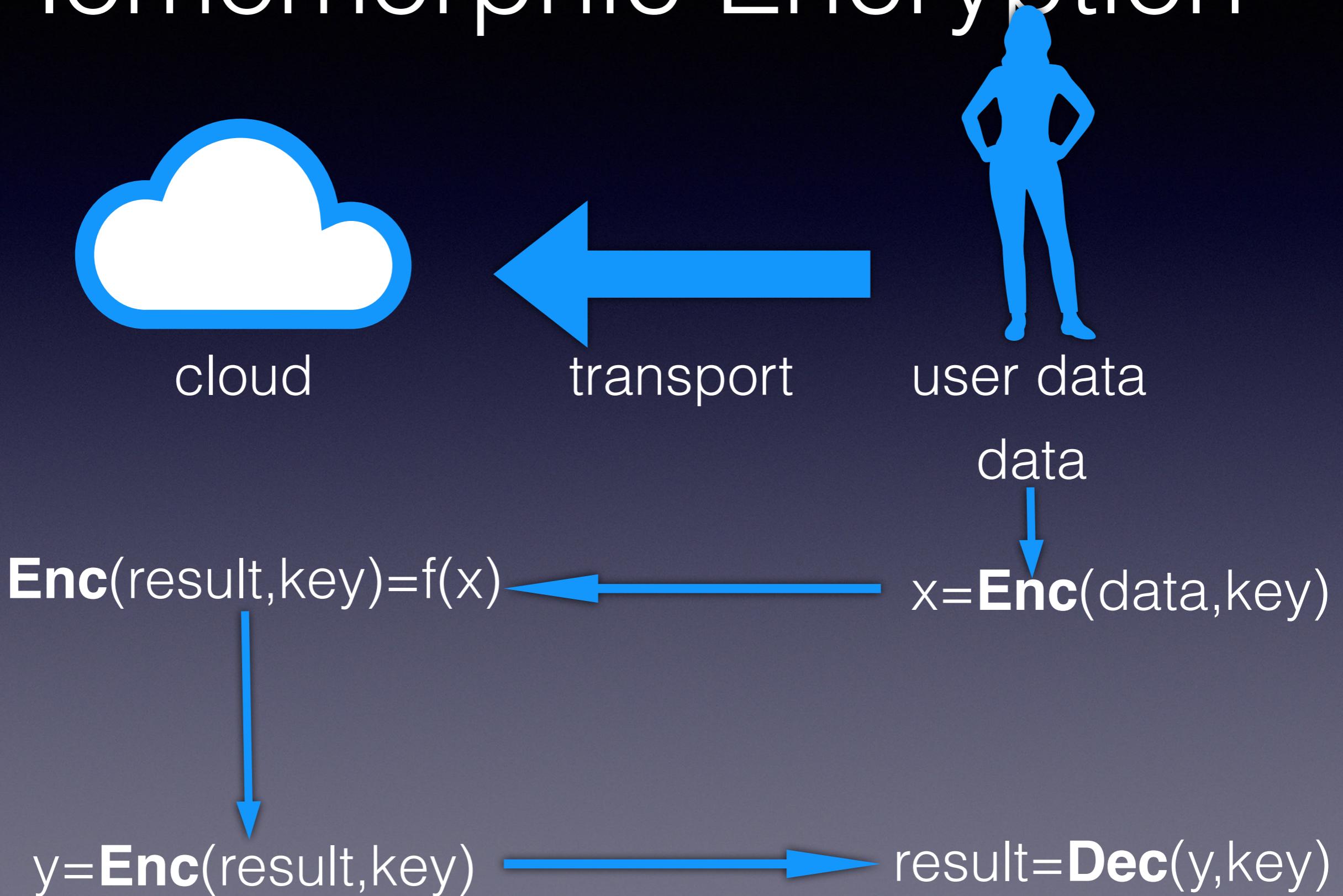
Homomorphic Encryption



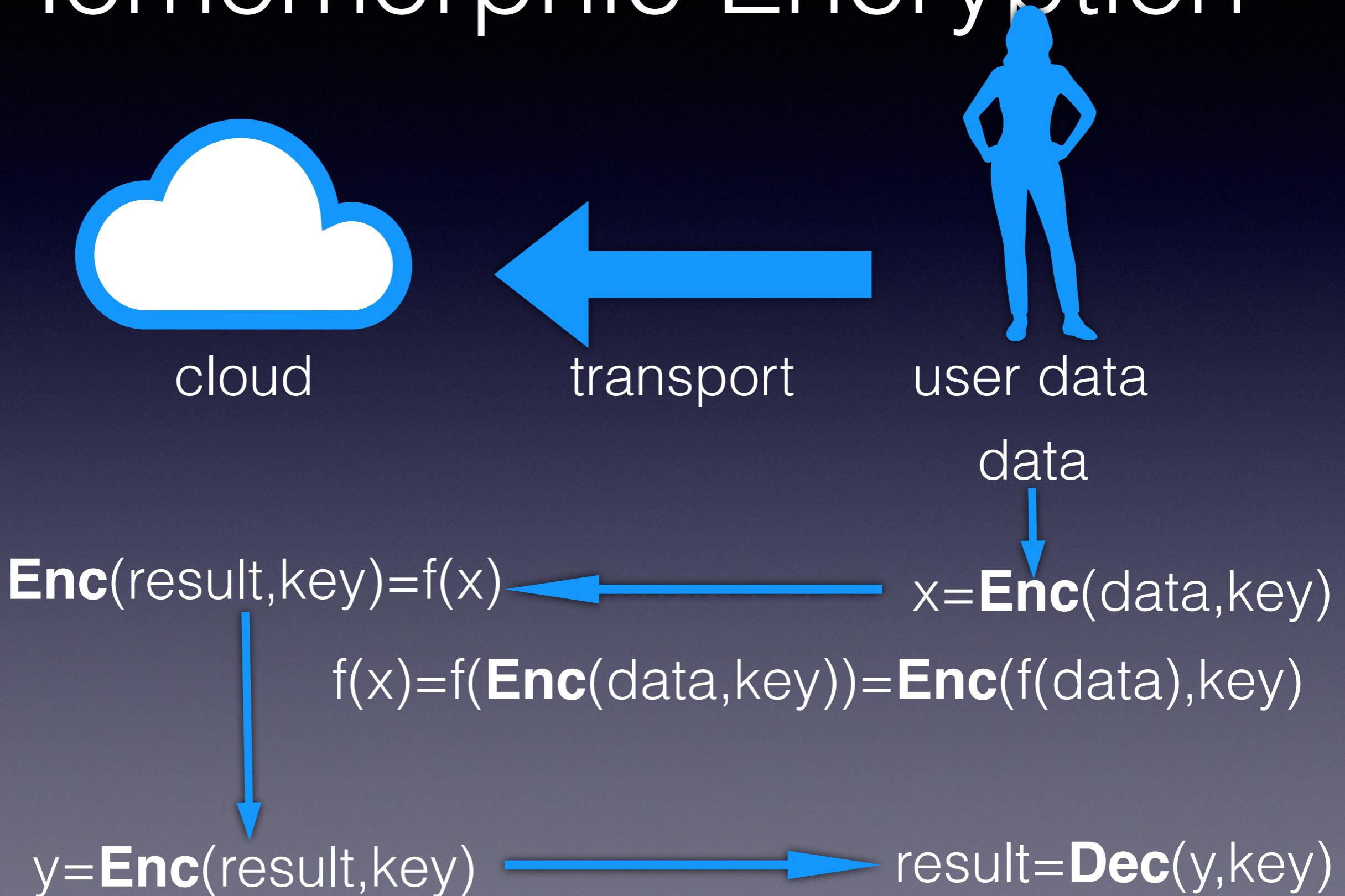
Homomorphic Encryption



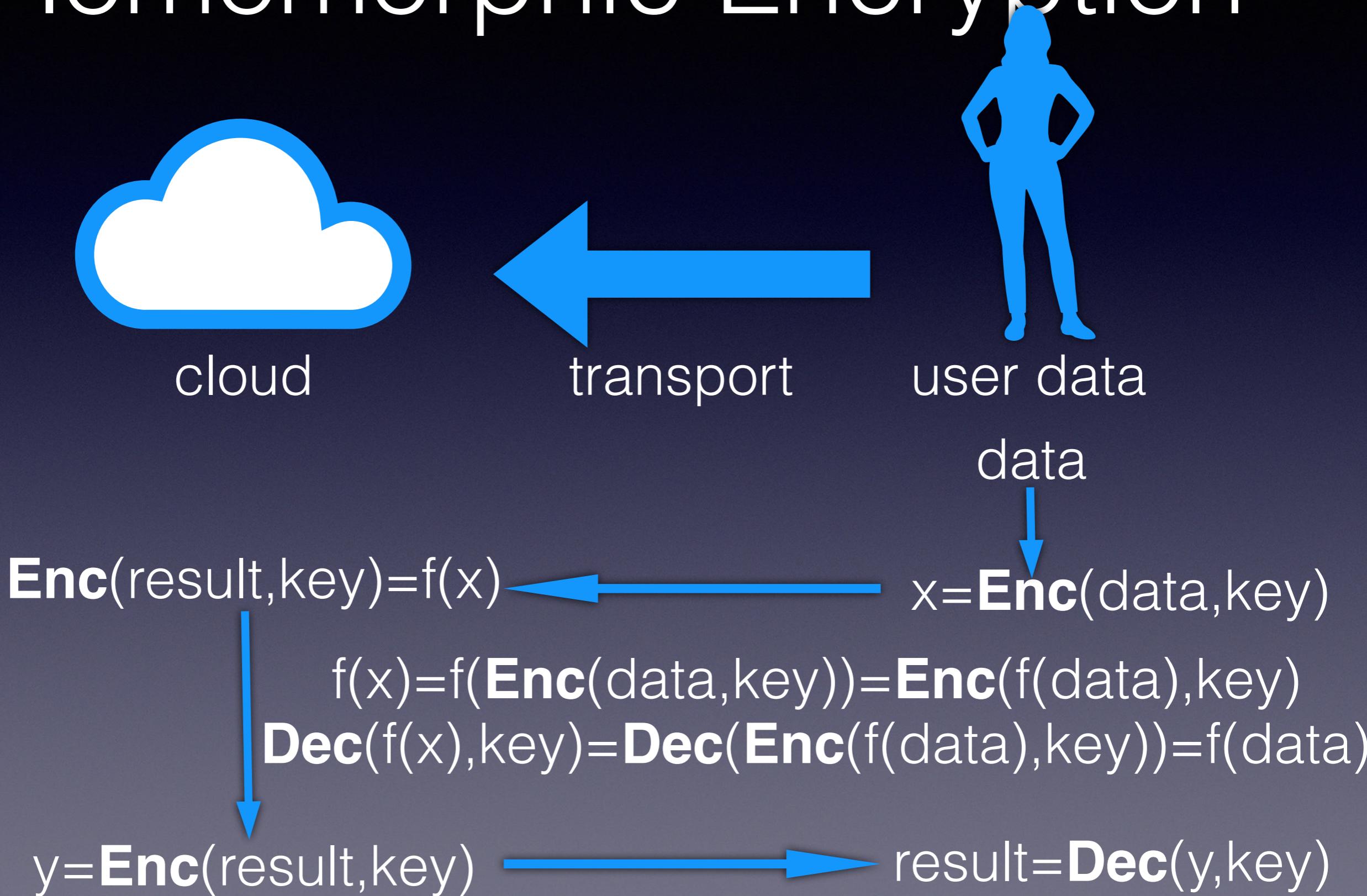
Homomorphic Encryption



Homomorphic Encryption



Homomorphic Encryption



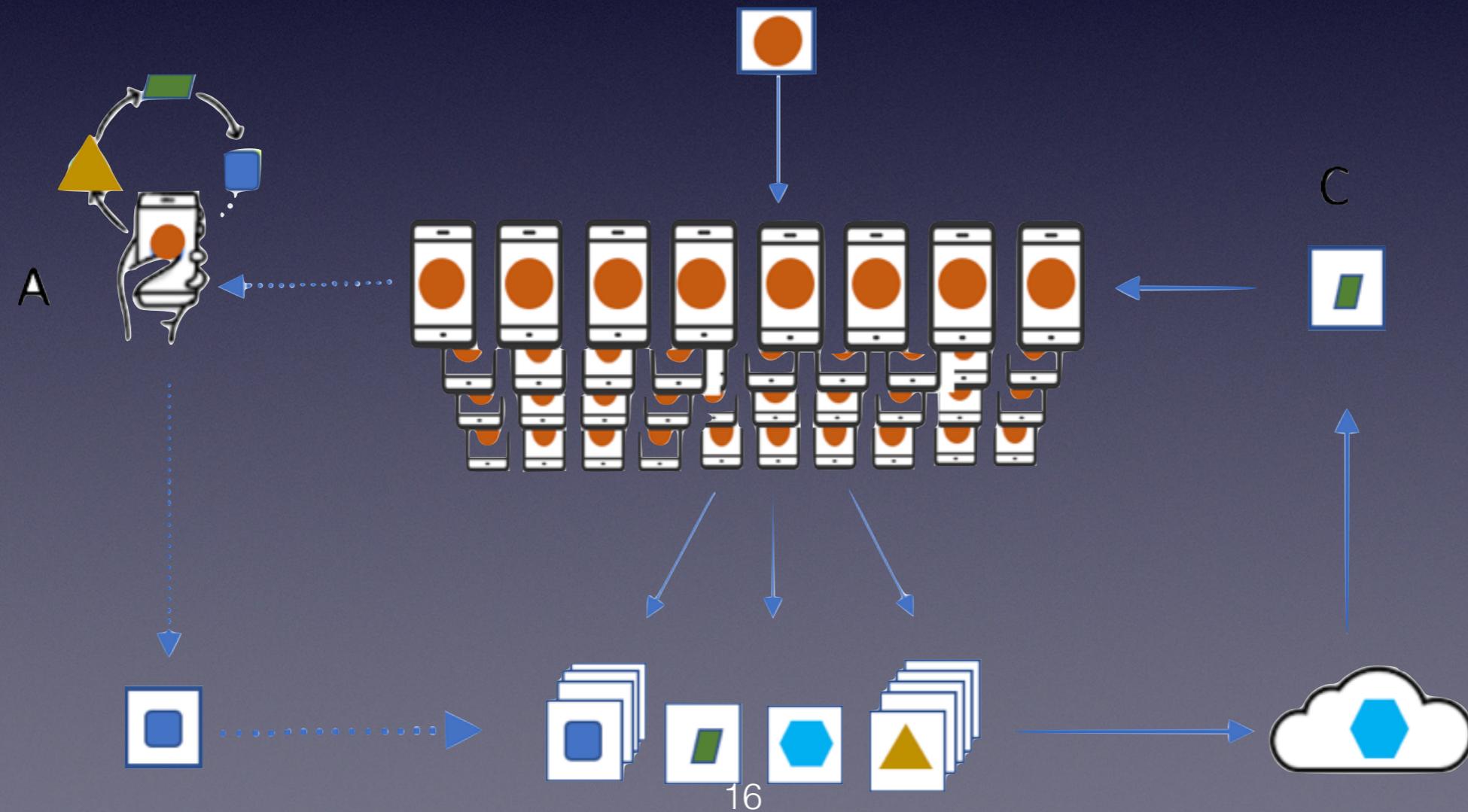
Esistono sistemi per HE

- Nel 1978 Rivest aveva posto la questione se fosse possibile trovare per qualsiasi funzione un crittosistema con la proprietà della HE:
$$\mathbf{Enc}(f(\text{data}), \text{key}) = f(\mathbf{Enc}(\text{data}, \text{key}))$$
- Negli anni sono state trovate funzioni f con la proprietà HE rispetto a particolari crittosistemi: addizione modulo 2, addizione con interi piccoli e moltiplicazione modulo p (ElGamal1984), addizione di interi grandi (Paillier1999), successore e moltiplicazione (Brakerski et al. 2005).

Federated Learning

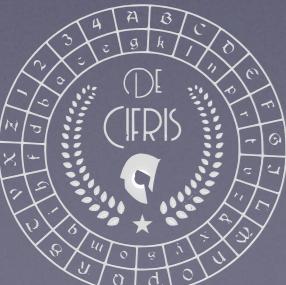
I modelli di Machine Learning (ML) invece di essere elaborati su grandi server di calcolo centralizzati vengono distribuiti sui dispositivi mobili.

Questo schema di calcolo benché teorizzato nel passato non è stato finora praticamente realizzato a causa dello scarso potere computazionale dei dispositivi mobili nell'ambito del ML. Milioni di dispositivi mobili sono ora provvisti di un coprocessore dedicato all'AI.



Differential Privacy

- Un algoritmo A randomizzato con parametro di controllo n implementa una funzione f in modo **differentially private** quando per ogni n e per ogni coppia di input x, x' (a distanza 1) si ha
$$h(A(x,n)) - h(A(x',n)) < 1/n$$
- $h(c)$ indica il contenuto informativo grezzo di una variabile aleatoria c.



Grazie!



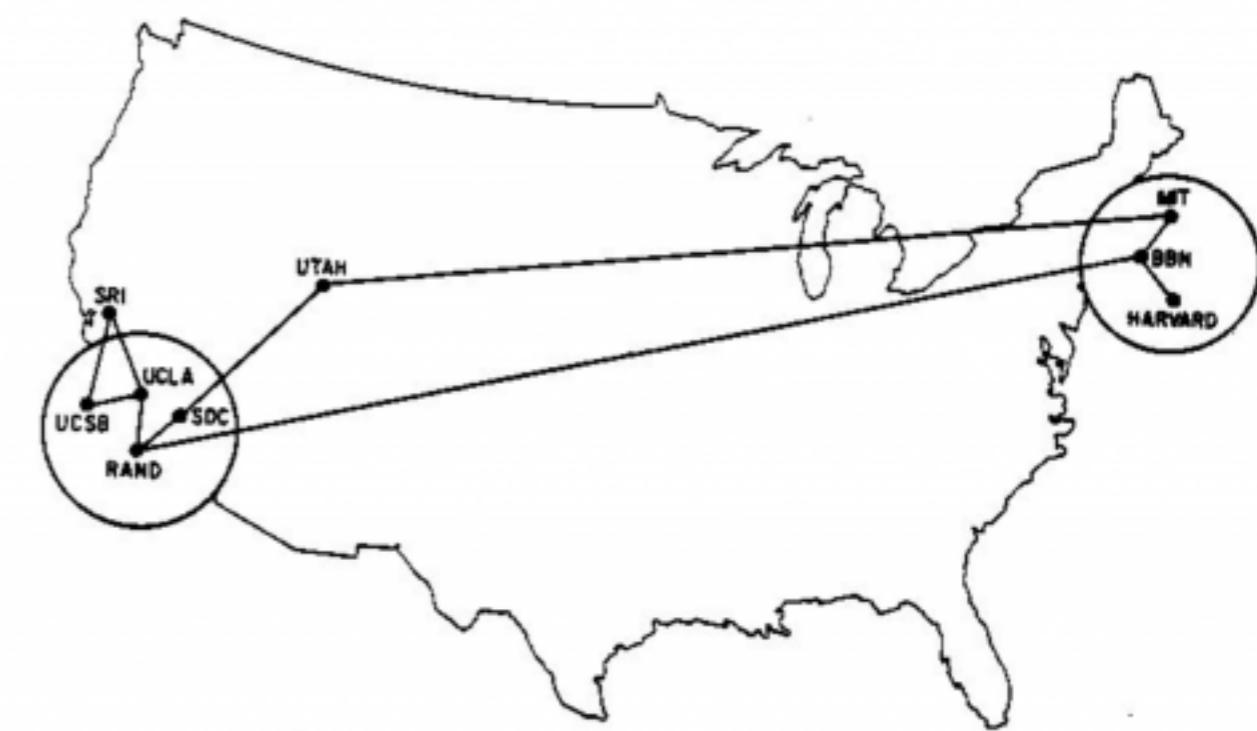
Riferimenti

- A. Shamir (1984) **Identity-Based Cryptosystems and Signature Schemes**
- Y. Dodis-L. Reyzin-A. Smith (2007) **Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data**
- C. Shannon (1948) **A Mathematical Theory of Communication**
- C. Shannon (1949) **Communication Theory of Secrecy Systems**
- A. Shamir (1979) **How to Share a Secret**
- O. Rabin (1981) **How to Exchange Secrets**
- S. Goldwasser-S. Micali (1982) **Probabilistic encryption and how to play mental poker keeping secret all partial information**
- Ling-Tzeng (2005) **An Efficient Solution to the Millionaires' Problem Based on Homomorphic Encryption**
- A.C. Yao (1982) **Protocols for secure computations**
- C.Dwork-F.McSherry-K. Nissim-A.Smith (2006) **Calibrating Noise to Sensitivity in Private Data Analysis**
- C. Crépeau (1997) **Efficient Cryptographic Protocols Based on Noisy Channels**
- D. Venturi (2012) **Crittografia nel Paese delle Meraviglie**
- M. Blum (1983) **Coin Flipping by Telephone a protocol for solving impossible problems**
- P. Paillier (1999) **Public-Key Cryptosystems Based on Composite Degree Residuosity Classes**
- T. ElGamal (1994) **A Public-Key Cryptosystem an a Signature Scheme Based on Discrete Logarithms**
- R. L. Rivest, L. Adleman, M. L. Dertouzos (1978) **On data banks and privacy homomorphisms**
- C. Gentry (2009) **Fully homomorphic encryption using ideal lattices**

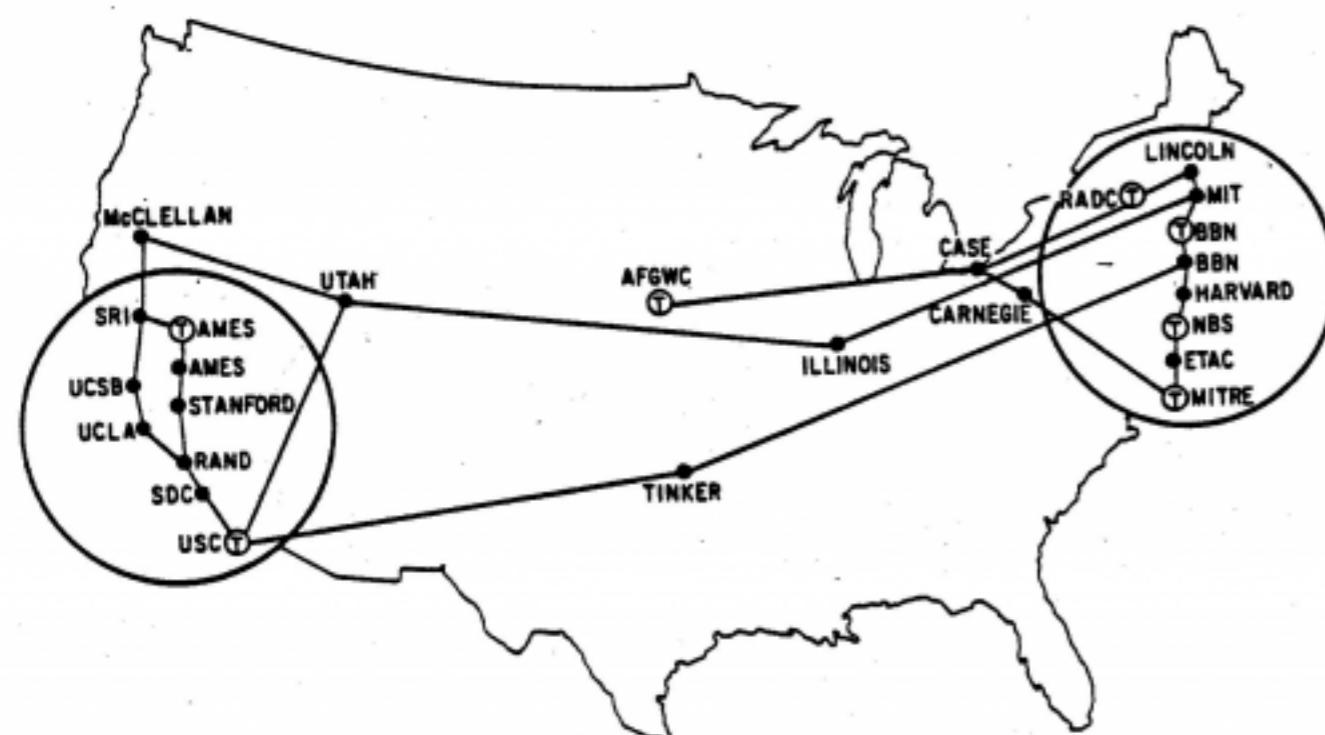




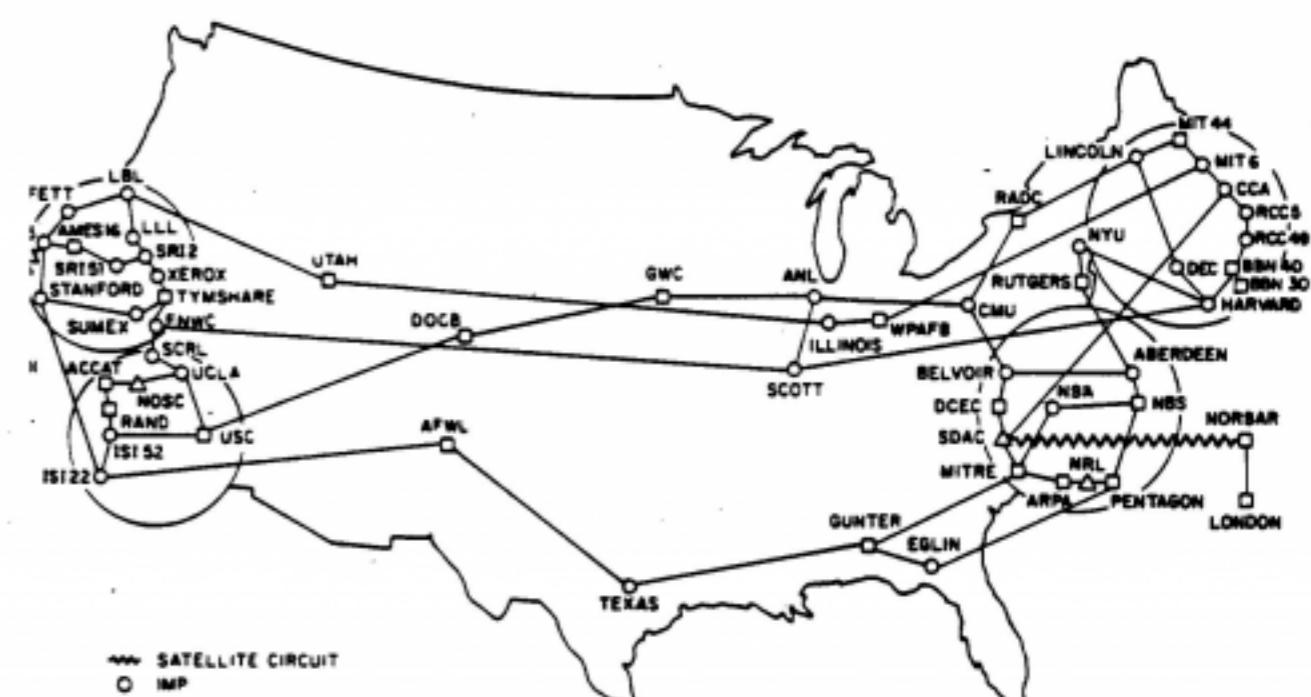
Dezember 1969



Juni 1970



März 1972



Juli 1977

1975

СЕВЕРНАЯ АМЕРИКА
СОЕДИНЕНИЯ СЕТИ
СОВЕТСКОГО ИССЛЕДОВАНИЯ
СОВЕТСКИХ СОЮЗОВ
СОВЕТСКОЙ АМЕРИКИ