Una famiglia di chiavi deboli nel Bitcoin

Domenica Sogiorno

ITASEC20
CRYPTANALYSIS: a key tool in securing and breaking ciphers

Ancona, 04.02.2020

Introduzione

- Sistema Bitcoin
- La crittografia utilizzata nel sistema Bitcoin, lo rende sicuro?
- Progetto nell'ambito di uno stage del Dipartimento di Matematica di Bari svoltosi presso il Dipartimento di Matematica di Trento

Tecnologia blockchain

- Sistema Bitcoin, 2008, prima applicazione della tecnologia blockchain.

  La blockchain = sistema di registro digitale immutabile utilizzato in reti distribuite.
  Consente lo scambio di risorse digitali attraverso la pubblicazione di transazioni in un registro pubblico.

La rete Bitcoin è:

- **totalmente decentralizzata**,
- **peer-to-peer**.

Utente Bitcoin:

- connessione Internet;
- portafoglio Bitcoin:
  - chiave pubblica o indirizzo Bitcoin,
  - chiave privata.

Affinché ci sia scambio di bitcoin è necessario pubblicare le cosiddette transazioni in un registro.

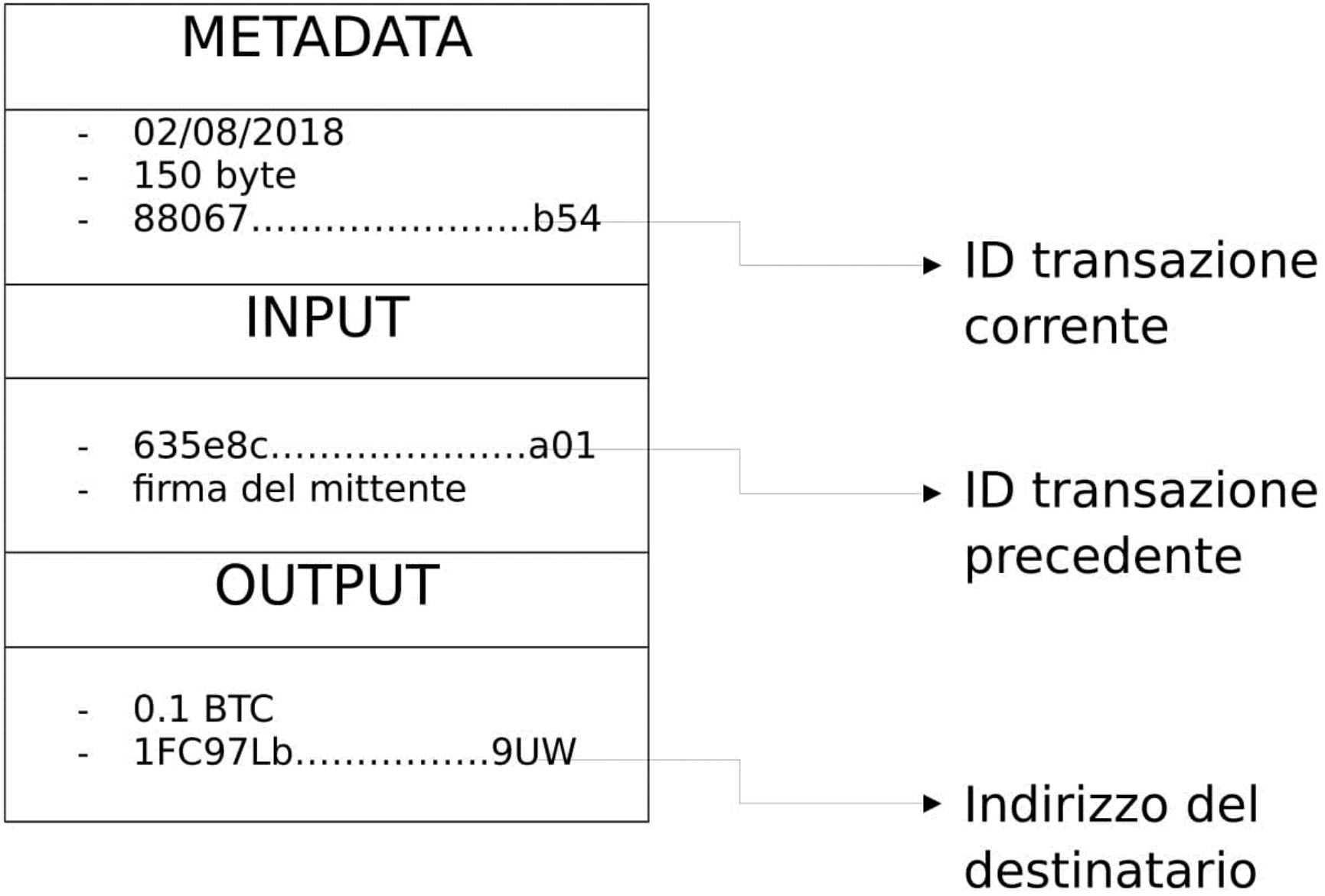
La rete Bitcoin è:

- **totalmente decentralizzata**,
- **peer-to-peer**.

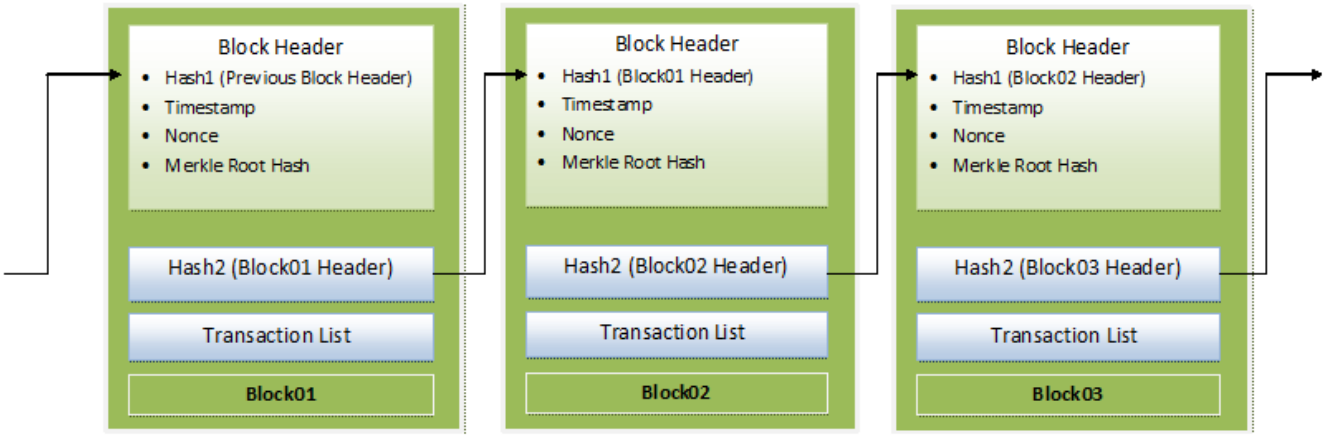
Utente Bitcoin:

- connessione Internet;
- portafoglio Bitcoin:
  - chiave pubblica o indirizzo Bitcoin,
  - chiave privata.

Affinché ci sia scambio di bitcoin è necessario pubblicare le cosiddette transazioni in un registro.


METADATA
- 02/08/2018
- 150 byte
- 88067.....b54
INPUT
- 635e8c.....a01
- firma del mittente
OUTPUT
- 0.1 BTC
- 1FC97Lb.....9UW
ID transazione corrente
ID transazione precedente
Indirizzo del destinatario

- Transazione corretta,
- gruppo di transazioni,
- creazione del blocco ⟵ Mining-"Proof of Work Consensus Model"
- pubblicazione del blocco.



È possibile, a partire da un indirizzo Bitcoin, calcolare la chiave privata e dunque impossessarsi dei bitcoin contenuti nel portafoglio corrispondente?

L'algoritmo che genera gli indirizzi Bitcoin è sicuro?

Definizione

Una funzione hash è una funzione matematica che prende in input una stringa di bit di lunghezza arbitraria e restituisce in output una stringa di lunghezza fissa, chiamata digest.

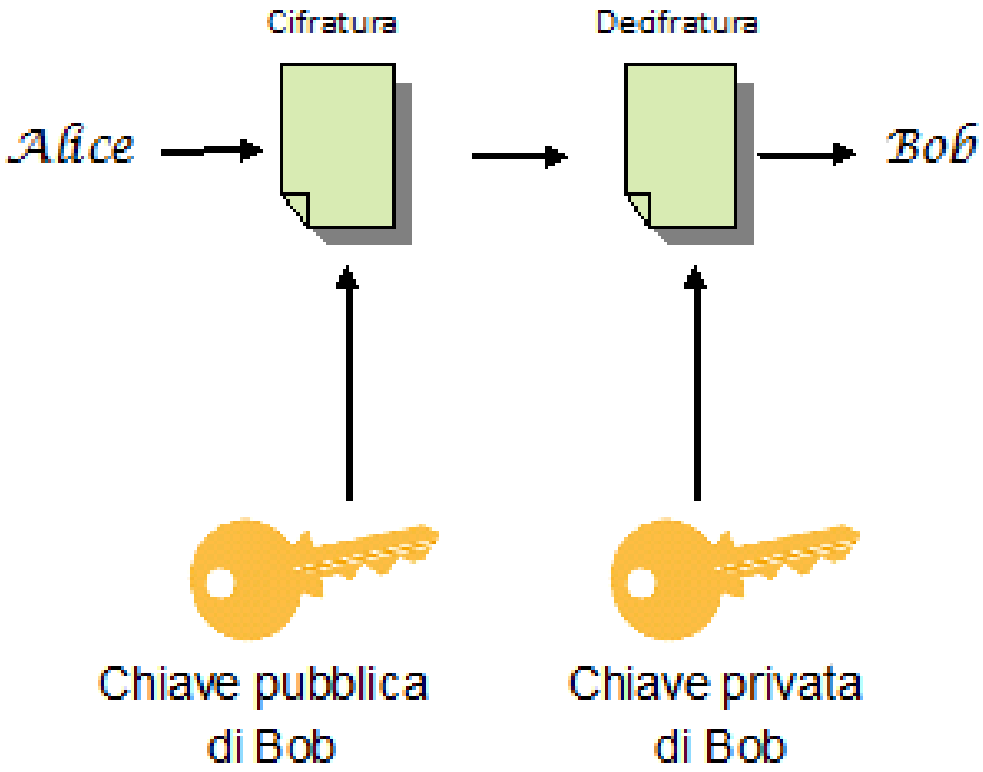
Problema 1 **"Collision"**: data una funzione hash $h : X \to Y$ trovare $x, x' \in X$, $x \neq x'$, tali che $h(x) = h(x')$.
Problema 2 **"Preimage"**: data una funzione hash $h : X \to Y$ e dato $y \in Y$ trovare $x \in X$ tale che $h(x) = y$.
Problema 3 **"Second Preimage"**: data una funzione hash $h : X \to Y$ e dato $x \in X$ trovare $x' \in X$, $x \neq x'$, tale che $h(x) = h(x')$.

Definizione

Una funzione hash è una funzione matematica che prende in input una stringa di bit di lunghezza arbitraria e restituisce in output una stringa di lunghezza fissa, chiamata digest.

Problema 1 **"Collision"**: data una funzione hash $h : X \to Y$ trovare $x, x' \in X$, $x \neq x'$, tali che $h(x) = h(x')$.
Problema 2 **"Preimage"**: data una funzione hash $h : X \to Y$ e dato $y \in Y$ trovare $x \in X$ tale che $h(x) = y$.
Problema 3 **"Second Preimage"**: data una funzione hash $h : X \to Y$ e dato $x \in X$ trovare $x' \in X$, $x \neq x'$, tale che $h(x) = h(x')$.

- **Crittografia a chiave pubblica.** L'idea alla base della crittografia a chiave pubblica è stata introdotta nel 1976 nell' Università di Standford dal professor Martin Hellman e dal suo studente Whitfield Diffie; loro hanno descritto come due parti possano comunicare in sicurezza su un canale insicuro senza condividere alcuna chiave.



Definizione

Si consideri K un campo di caratteristica diversa da 2 e da 3, e un polinomio di terzo grado $x^3 + ax + b$ $(a, b \in K)$ che abbia radici tutte distinte. Si definisce curva ellittica non singolare l'insieme

$$E = \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b,\ a, b \in K\} \bigcup \{\mathcal{O}\}$$

cioè l'insieme delle soluzioni $(x, y) \in K \times K$ dell'equazione $y^2 = x^3 + ax + b$ più un punto speciale chiamato punto all'infinito $\mathcal{O}$.

Data E una curva ellittica non singolare, si definisce su essa un'operazione binaria che rende E un gruppo abeliano. Procediamo alla definizione nel caso $K = \mathbb{R}$, che fa riferimento alla rappresentazione geometrica della curva nel piano.

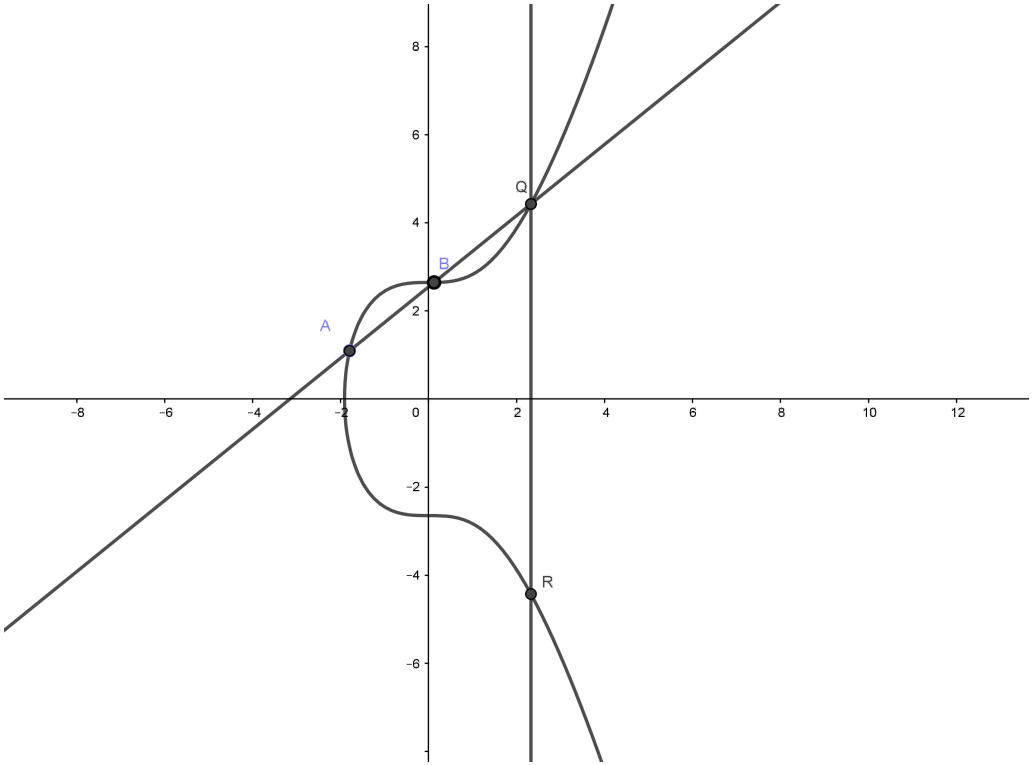
Definizione

Sia E una curva ellittica non singolare su $\mathbb{R}$. Si definisce l'operazione

$$+ : E \times E \to E$$

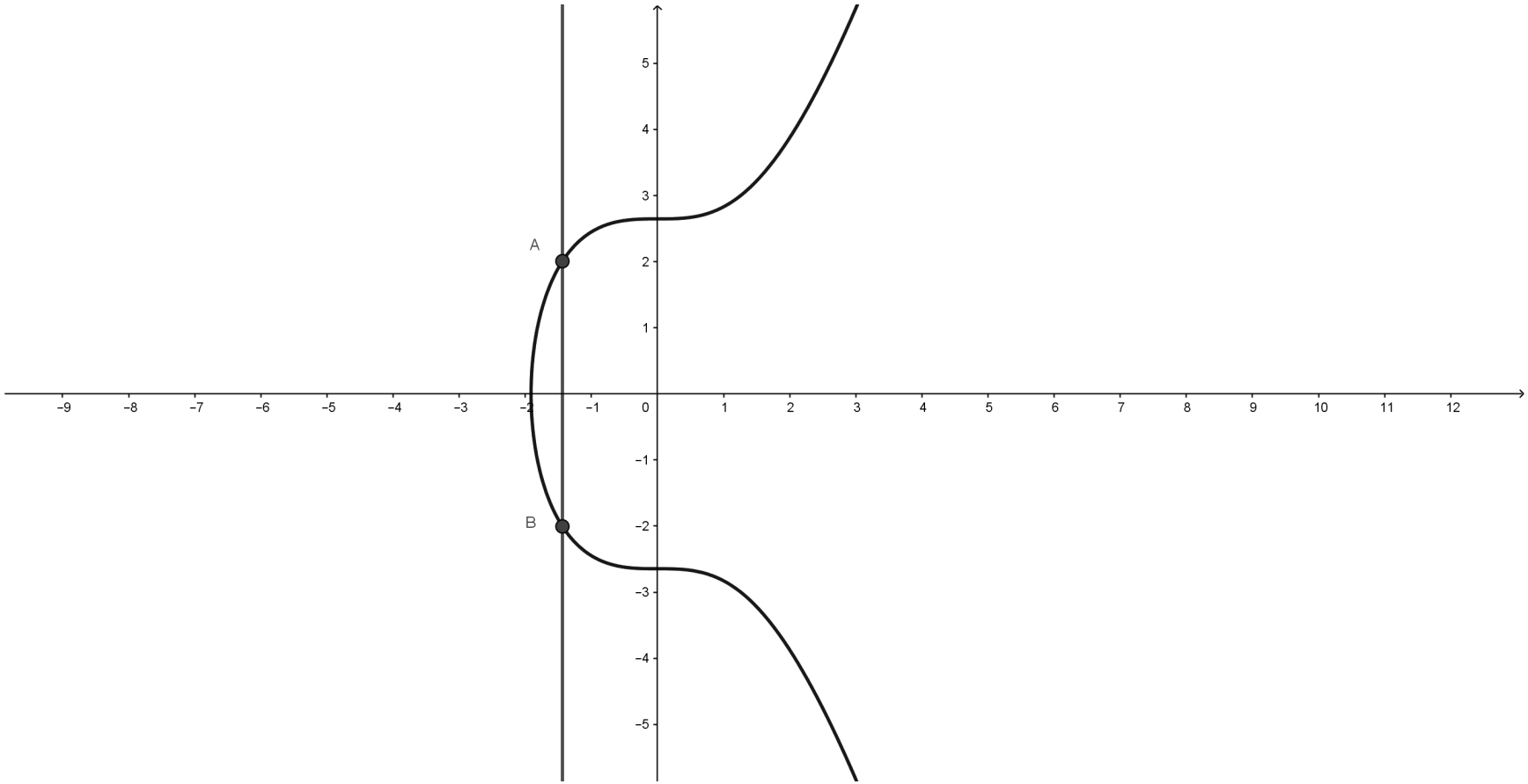
Dati $A = (x_1, y_1)$, $B = (x_2, y_2) \in E$:

- *se $x_1 \neq x_2$: $A + B = R$*



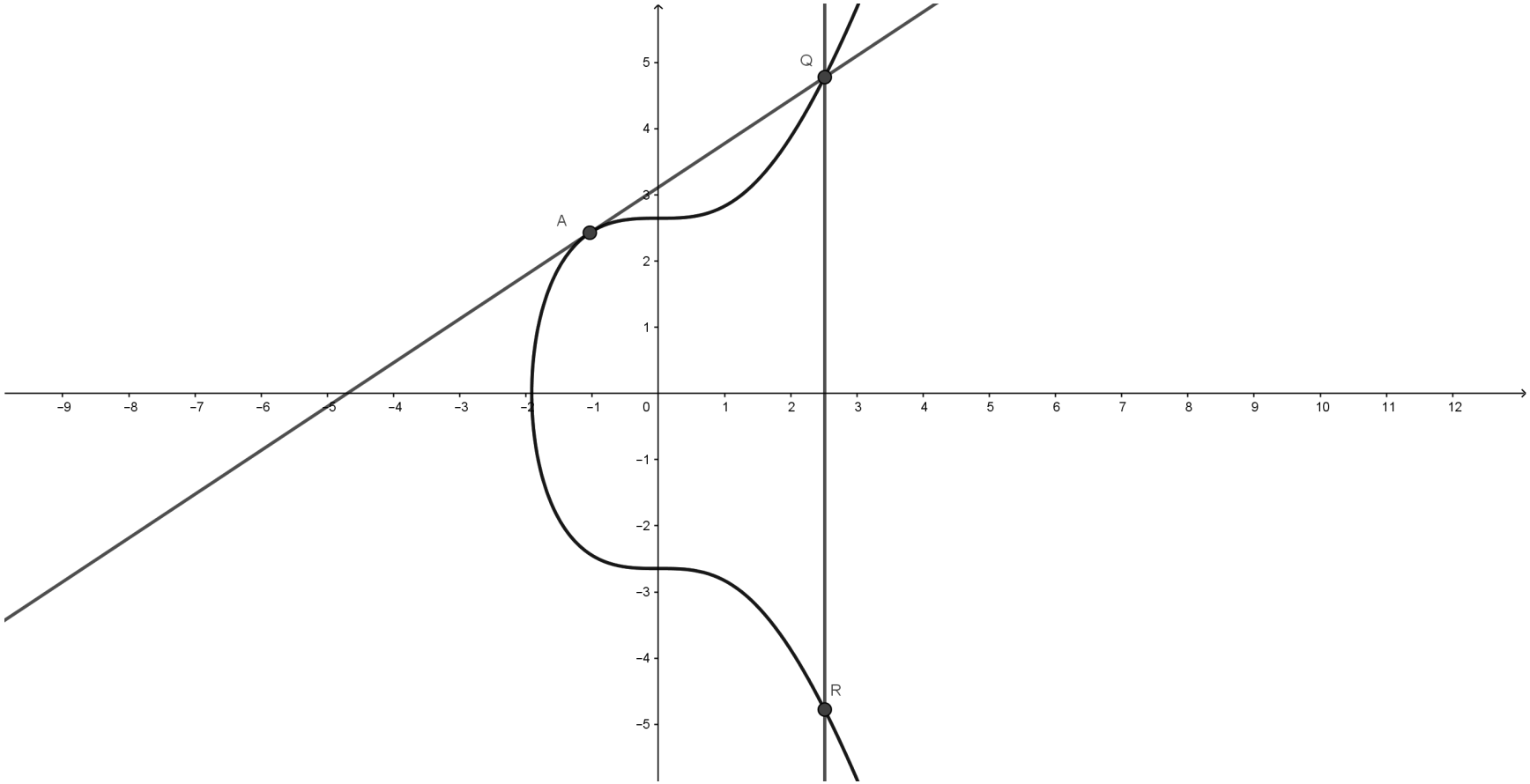
Definizione

- $se\ x_1 = x_2\ e\ y_1 = -y_2 : A + B = \mathcal{O}$



Definizione

- *se* $x_1 = x_2$ *e* $y_1 = y_2$*:* $A + B = R$



Se i punti coincidono e il punto è sull'asse x: $2A = \mathcal{O}$ *da cui* $A = -A$*.*

Proposizione

$(E, +)$ è un gruppo abeliano con elemento neutro $\mathcal{O}$.

Definizione

Preso k un numero naturale e P un punto di una curva ellittica E,

$$kP := \underbrace{P + P + P + \cdots + P}_{k}$$

Per definizione se $k = 0$ allora $0 \cdot P = \mathcal{O}$ per ogni P sulla curva.
Se $k < 0 \Rightarrow kP = \mid k \mid [-P]$.
Dato un punto P di una curva ellittica E si definisce ordine del punto, se esiste, il più piccolo $m \neq 0$ positivo tale che $mP = \mathcal{O}$.
Se tale m non esiste si dice che P ha ordine infinito.
Curve ellittiche definite su campi finiti non ammettono punti di ordine infinito.

Definizione (Problema del logaritmo discreto per curve ellittiche)

Considerata una curva ellittica E su un campo K e due punti P e Q su E, con P di ordine n e $Q \in < P >$, si vuole trovare lo scalare k tale che $Q = kP$.

Funzione one-way: multiplo di un punto.

Osservazione

- *P è chiamato **punto base**.*
- *In crittografia si prendono generalmente curve di ordine un primo grande, così che:*
  - *ogni punto della curva sia generatore,*
  - *lo spazio di chiavi sia più grande possibile.*

Generazione indirizzi Bitcoin

La curva ellittica usata dal sistema Bitcoin è la cosiddetta *Secp*256*k*1, secondo la classificazione *Standards for Efficient Cryptography (SEC)* ed è definita a partire dall'equazione di Weierstrass con i parametri $a = 0$ e $b = 7$:

$$y^2 = x^3 + 7$$

$K = F_p$ con

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1.$$

Il punto base è $P = (P_x, P_y)$, che in forma esadecimale è

$P_x =$ 79*BE*667*E* *F*9*DCBBAC* 55*A*06295 *CE*870*B*07 029*BFCDB*
2*DCE*28*D*9 59*F*2815*B* 16*F*81798

$P_y =$ 483*ADA*77 26*A*3*C*465 5*DA*4*FBFC* 0*E*1108*A*8 *FD*17*B*448
*A*6855419 9*C*47*D*08*F* *FB*10*D*4*B*8.

- Preso $1 \leq k \leq N-1$ si calcola la chiave pubblica $Q = k \cdot P$.
  E è un gruppo finito, #E è il numero primo:

$$q = 1157920892373161954235709850086879078528375$$
$$642790749043826051631415181614943 37$$

  E è ciclico e $ord(P) = q$.
  Spazio delle chiavi private: $\mathbb{Z}_q{}^*$.

- RIPEMD-160, SHA-256

- codifica in Base58

- Preso $1 \leq k \leq N-1$ si calcola la chiave pubblica $Q = k \cdot P$.
  E è un gruppo finito, #E è il numero primo:

$$q = 115792089237316195423570985008687907852837564279074904382605163141518161494337$$

  E è ciclico e $ord(P) = q$.
  Spazio delle chiavi private: $\mathbb{Z}_q{}^*$.

- RIPEMD-160, SHA-256

- codifica in Base58

- Preso $1 \leq k \leq N-1$ si calcola la chiave pubblica $Q = k \cdot P$.
  E è un gruppo finito, #E è il numero primo:

$$q = 115792089237316195423570985008687907852837564279074904382605163141518161494337$$

  E è ciclico e $ord(P) = q$.
  Spazio delle chiavi private: $\mathbb{Z}_q{}^*$.

- RIPEMD-160, SHA-256

- codifica in Base58

Tornando alla domanda . . .
L'algoritmo che genera gli indirizzi Bitcoin è sicuro?

In linea generale si:

- complessità esponenziale del problema del logaritmo discreto su $Secp256k1$
- No attacco brute force

Progetto stage: Attuare un attacco brute force su un sottogruppo H del gruppo $\mathbb{Z}_q{}^*$, con un numero di elementi non troppo grande.

Tornando alla domanda . . .
L'algoritmo che genera gli indirizzi Bitcoin è sicuro?

In linea generale si:

- complessità esponenziale del problema del logaritmo discreto su $Secp256k1$
- No attacco brute force

Progetto stage: Attuare un attacco brute force su un sottogruppo H del gruppo $\mathbb{Z}_q{}^*$, con un numero di elementi non troppo grande.

Tornando alla domanda . . .
L'algoritmo che genera gli indirizzi Bitcoin è sicuro?

In linea generale si:

- complessità esponenziale del problema del logaritmo discreto su $Secp256k1$
- No attacco brute force

Progetto stage: Attuare un attacco brute force su un sottogruppo H del gruppo $\mathbb{Z}_q{}^*$, con un numero di elementi non troppo grande.

Costruzione del sottogruppo H

Data la fattorizzazione di $q-1$:

$$q-1 = 2^6 \cdot 3 \cdot 149 \cdot 631 \cdot \underbrace{10736179381659537}_{p_1} \cdot \underbrace{174723607534414371449}_{p_2}$$

$$\cdot \underbrace{3419484869741660005223436092831 89}_{p_3}$$

preso t primitivo in $\mathbb{Z}_q^*$ $(t = 7)$ e $w = p_1 \cdot p_2 \cdot p_3$

$$H =< t^w >= \{t^{wi}, i \in [0, 18051647]\}$$

di ordine $2^6 \cdot 3 \cdot 149 \cdot 631 = 18051648$.

Costruzione del sottogruppo H

Data la fattorizzazione di $q-1$:

$$q-1 = 2^6 \cdot 3 \cdot 149 \cdot 631 \cdot \underbrace{107361793816595537}_{p_1} \cdot \underbrace{174723607534414371449}_{p_2}$$

$$\cdot \underbrace{341948486974166000522343609283189}_{p_3}$$

preso t primitivo in $\mathbb{Z}_q{}^*$ $(t = 7)$ e $w = p_1 \cdot p_2 \cdot p_3$

$$H =< t^w >= \{t^{wi}, i \in [0, 18051647]\}$$

di ordine $2^6 \cdot 3 \cdot 149 \cdot 631 = 18051648$.

Prima fase del progetto

- Generazione di indirizzi Bitcoin con chiavi private in H
- controllo dell'eventuale presenza di tali indirizzi nella blockchain

---

p; E=EllipticCurve([GF(p)|0,0,0,0,7]); q:= #E; w:= $p_1 \cdot p_2 \cdot p_3$;
t :=PrimitiveElement(GF(q)); g:= t^w;
for i in range do
$d := g^i$;
Write("RisIndirizzi", AdGen(d));
end for;
Bitcoinscrape.py: preso in input un file con indirizzi Bitcoin verifica la presenza di questi nella blockchain facendo riferimento al sito *https://blockchain.info*

Seconda fase del progetto

Esiti positivi: 4 indirizzi Bitcoin da noi generati realmente esistenti

1. 1PSRc.....y4yqPQ3
2. 1B5US.....cLQ4wCt
3. 1JPbz.....D5uha5m
4. 1EHNa.....hwF6kZm

Abbiamo creato un portafoglio Bitcoin a nome del Cryptolab e, dopo averlo caricato, abbiamo spostato 0.0002 BTC (1.3 USD) da questo all'indirizzo 1PSRcas.....yqPQ3; dopo qualche istante abbiamo restituito i bitcoin al nostro indirizzo, sfruttando la chiave privata dell'indirizzo forzato.

Seconda fase del progetto

Esiti positivi: 4 indirizzi Bitcoin da noi generati realmente esistenti

1. 1PSRc.....y4yqPQ3
2. 1B5US.....cLQ4wCt
3. 1JPbz.....D5uha5m
4. 1EHNa.....hwF6kZm

Abbiamo creato un portafoglio Bitcoin a nome del Cryptolab e, dopo averlo caricato, abbiamo spostato 0.0002 BTC (1.3 USD) da questo all'indirizzo 1PSRcas.....yqPQ3; dopo qualche istante abbiamo restituito i bitcoin al nostro indirizzo, sfruttando la chiave privata dell'indirizzo forzato.

Grazie per l'attenzione