- Bob takes cash to bank to get money
- Alice spends cash with Bob (offline)

Bank (not convenient)

Alice buys an unit of cash from

Digital cash
Getting back from work

Alice puts blind spot on

Access 0/1

Send # etc.

volume, etc.

< signed by bank

$2 to kids

Count $5, $1, $2

1 2 3 4
A new sense seemed to begin.
A sense of the sea
From tables of data.
\[ E_k(x, y(x)) = \text{count}(x) \]

- All new keys
- Path shaves recovered
- Path verifiable

Next column
200 blocks

BEDs also Alice for
Bob takes everything & gives to Bank

→ Bank can do same verification that Bob did

↓ DOUBLE SPENT

→ check the 2 cash units

→ all reveals same

→ Bob guilty

→ some reveals are left & some R

→ Alice’s ID revealed
discrete log on finite fields

- based on difficulty of

\[ 3072 \text{ bit RSA} \]

\[ 256 \text{ bit ECC} \]

\[ 128 \text{ bit AES} \]

- shorter keys

Advantages

Elliptic Curve Cryptography (ECC)

Public key/Asymmetric
Use number on an elliptic curve

\[ y^2 = x^3 + ax + b \]

\[ \text{known} \]

\[ \text{constant} \]
Reflect 

Find intersection 

Draw a line 

Addition (a+b)

(\text{some}) 
L, \text{line} = \text{tangent} 
(a+4a) = 2a 

Also 

Reflect 

Compute 

If is
ECC 500 Finite Field (mod n)
Some graphs of elliptic curves
In order to be in order, should be in order of a sequence also. Mediation of a sequence +

define a curve F generator → a, b, n, g
Given a, b ∈ C, we cannot find if

compute \( ab = a + b + \cdots \) then

choose a (point on curve)

Design key properly
Is $F_p < \text{comp and react?}$

Find $y$.

Given $x$. 

[Diagram with labeled points and lines]
ECC key exchange (ECC-DH)

Alice chooses a

\[ g \times A = B \]

Bob chooses \( g \times B = A \)

...
key exchange & authentication

Alice shares her F_A with Bob.

Sign F_A by C_A

Alice's public key = F_A

We RSA certificates (?)
Curve P-192

$y^2 = x^3 - 3c + B$

Modulus = (in decimal)
6277101 \times 63101 \times 662465 \times 7379791

$B = 64210519 \times e59c80e7 \times 0fa7e9ab \times 72243049 \times feb8deec$

$G = Gx, Gy$

$G = 188da80e \times b03090f6 \times 7cbf20e \times b43a1880 \times 82ff0afd \times 82ff1012$

$G = Gx, Gy$

$c146b961$

$G = 64210519 \times e59c80e7 \times 0fa7e9ab \times 72243049 \times feb8deec$

$B = 1e794811$

Modulus = (in decimal)

$y^2 = x^3 - 3c + B$

Curve P-192