Hash functions

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Emai: gianluca.dini@unipi.it
Version: 01/04/2025

1

An example

The input size is finite but arbitrary

```
Nel mezzo del cammin di nostra vita
mi ritrovai per una selva oscura
che' la diritta via era smarrita.

Ahi quanto a dir qual era e` cosa dura
esta selva selvaggia e aspra e forte
che nel pensier rinova la paura!
```

MD5

```
0xd94f329333386d5abef6475313755e94
```

128 bit

The hash size is fixed, generally smaller than the message size

2

Informal properties

- Applicable to messages of any size
- Output of fixed length (digest, hash, fingerprint, tag,…)
- No key (!)
- "Easy" to compute
- "Difficult" to invert (it is not invertible. But must be hard to go back)
- "Unique": the hash of a message can be used to "uniquely" represent the message Not possible by definition

3

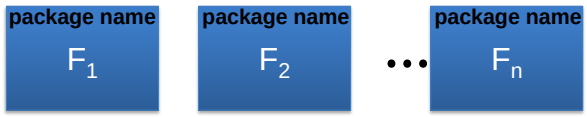
Informal properties

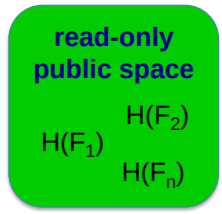
- The fingerprint must be *highly* sensitive to *all* input bits
- if we make minor modifications to the input, the output should look like very different
- Example
  - Input «I am not a crook»
    - Hash (MD5): 6d17fcd4ae0e82fa4409f4ea6f4106a6
  - Input «I am not a cook»
    - Hash (MD5): 9ebe3d42d5c01fc59fe3daacbf42f515
- https://www.fileformat.info/tool/hash.htm

4

Example: protecting files

- **Software packages**





- When user downloads package, can verify that contents are valid
  - An attacker cannot modify a package without detection
- No key needed (public verifiability), but requires read-only space

5

Example: protecting files

6

Properties and collisions

- A hash function H: $\{0,1\}^* \rightarrow \{0,1\}^n$ Since # inputs are much larger than # of outputs, we have collisions
- **Properties**
  - **Compression**: H maps an input *x* of arbitrary finite length into an output H(x) of fixed length *n*
  - **Ease to compute:** given *x*, H(x) must be "easy" to compute
  - **Many-to-one:** a hash function is many-to-one and thus implies collisions (pigeonhole principle)
- (**Def**) A **collision** for H is a pair x_1, x_2 s.t. $H(x_1) = H(x_2)$ and $x_1 \neq x_2$

Security properties [1/2]

- **Preimage resistance (one-wayness)**
  - For essentially all pre-specified outputs, it is *computationally infeasible* to find any input which hashes to that output
    - i.e., given an output y, to find x such that y = h(x) for which x is not known (There are collisions, but function is not invertible)
- **2nd-preimage resistance (weak collision resistance)**
  - it is computationally infeasible to find any second input which has the same output as any specified input
    - i.e., given x, to find x' ≠ x such that h(x) = h(x')

Security properties [2/2]

- **Collision resistance (strong collision resistance)**
  - it is computationally infeasible to find any two distinct inputs which hash to the same output,
    - i.e., find x, x' such that $h(x) = h(x')$

↑ no input is given, while 2nd preimage resistance does. It's harder.

Point is, collisions are difficult to find, but so difficult that I can think of hash as something that does not have so.

Classification

- **One-way hash function (OWHF)** Nomenclature ↓
  - Provides preimage resistance, 2-nd preimage resistance
  - OWHF is also called weak one-way hash function
- **Collision resistant hash function (CRHF)**
  - Provides 2-nd preimage resistance, collision resistance
  - CRHF is also called strong one-way hash function

Relationship between security properties

- **FACT 1:** Collision resistance implies 2nd preimage resistance
- **FACT 2:** Collision resistance does not imply preimage resistance
  - However, in practice, CRHF almost always has the additional property of preimage resistance

11

Attacking Hash Functions

- An attack is successful if it produces a collision (**forgery**)
- Types of forgery
  - **Selective forgery**: the adversary has complete, or partial, control over x
  - **Existential forgery**: the adversary has no control over x

12

Black box attacks →

↳ does not exploit hash algorithm for the attack

- Consider H(·) as a black box
- Only consider the output bit length n
- Assume H(·) approximates a random variable
  - Each output is equally likely for a random input (so weak collisions exist for all output values)

Output length is limited to security and performance.
If hash is well defined, it approximates a random variable.

Specific Black box Attacks ↓

- **Guessing attack**
  - find a 2nd pre-image (Wants to violate 2nd property)
  - Running time: $O(2^n)$ hash ops
- **Birthday attack**
  - find a collision
  - Running time: $O(2^{n/2})$ hash ops More efficient: break collision resistance
- These attacks constitute a **security upper bound**
  - More efficient analytical attacks may exist (e.g., against MD5 and SHA-1)

In MD5, finding x_1, x_2 to get same hash was more efficient than Birthday attacks.

In 2017 also SHA-1 was compromised. Violate third property more efficiently than birthday attack. $n=160$, so $O(2^{n/2}) = O(2^{80})$

Guessing attack

→

- Objective: to find a 2nd pre-image
  - Given x_1, find $x_2 \neq x_1$ s.t. $H(x_1) = H(x_2)$
- The attack

```
int GuessingAttack(x1) {
    do
        x2 ← random(); // guessing
    while ( H(x1) != H(x2) )
    return x2;
}
```

Keep this until two values are the same

15

Guessing attack

↓

- Running time
  - Every step requires
    - 1 random number generation: efficient!
    - 1 hash function computation: efficient!
  - Constant and negligible data/storage complexity
  - Running time in the order of 2^n operations
    - At each step $Pr[H(x1) = H(x2)] = 1/2^n$

16

Birthday attack →

- Start with
  - x_1 = «Transfer $10 into Oscar's account»
  - x_2 = «Transfer $10.000 into Oscar's account»
- The attack
  - **do**
    - Alter x_1 and x_2 at non-visible locations so that semantics is unchanged (e.g., insert spaces, tabs, return,…)
  - **while** ($H(x_1)$!= $H(x_2)$)

17

Birthday attack →

- The birthday attack algorithm
  1. Choose $N = 2^{n/2}$ random input messages $x_1, x_2, \ldots, x_N$ (distinct w.h.p.)
  2. For $i := 1$ to N compute $t_i = H(x_i)$
  3. Look for a collision ($t_i = t_j$), $i \neq j$. If not found, go to step 1.
- Attack complexity
  - Running Time: $2^{n/2}$
  - Space: $2^{n/2}$
  - Probability of collision is 50%

18

Birthday paradox: intuition →

- Problem #1. Violating 2nd pre-image property is comparable to:
  - In a room of t = 23 people, what is the probability that at least a person is born on 25 December?
    - Answer: 0.063

SPECIFIC HASH

- Problem #2. Finding a collision is comparable to:
  - In a room of t = 23 people, what is the probability that at least 2 people have the same birthdate?
    - Answer: 0.507

19

Birthday attack →

- Apply the birthday paradox to hash function
  - We have: 2^n elements and t inputs (x_1, x_2, …, x_t)
  - π = Pr[no collision] = $\left(1-\frac{1}{2^n}\right)\left(1-\frac{2}{2^n}\right)\cdots\left(1-\frac{t-1}{2^n}\right) =$

$$\prod_{i=1}^{t-1}\left(1-\frac{i}{2^n}\right) \approx \prod_{i=1}^{t-1} e^{-\frac{i}{2^n}} = e^{-\frac{1+2+\cdots+t-1}{2^n}} \approx e^{-\frac{t(t-1)}{2^{n+1}}} \cong e^{-\frac{t^2}{2^{n+1}}}$$

20

Birthday attack →

- Probability of collision $\lambda = 1 - \pi$
- Solve in t, ➔ $t \approx 2^{(n+1)/2}\sqrt{\ln\left(\frac{1}{1-\lambda}\right)}$
- For $\lambda = 0.5$, $t \approx 1.2 \times 2^{n/2}$

Birthday attack ↓

- In practice,
  - The number of messages we need to hash to find a collision is in the order of the square root of the number of possible output values, i.e., $\sqrt{2^n} = 2^{n/2}$
- Example
  - n = 80 bit, $\lambda = 0.5$ ➔ $t \approx 2^{40.2}$ (doable with current laptops)
  - The probability of collision λ does not influence the attack complexity very much
- Rule of thumb: sizeof(digest) = 2 × sizeof(key)
  - Key is a block cipher key

Hash functions

HOW TO BUILD HASH FUNCTIONS

23

Types of hash functions

- Dedicated hash functions
- Block cipher-based hash functions

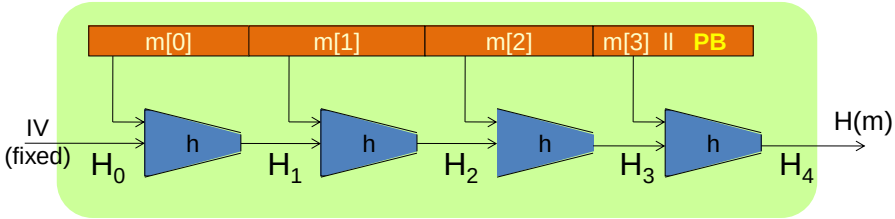
24

How to build a hash function

- Approach
  - Given a CRHF for short messages, construct a CRHF for long messages
- Solution:
  - The Merkle-Damgard iterated construction
  - Most of hash functions follow the Merkle-Damgard construction including SHA.

25

The Merkle-Damgard iterated construction



- Compression function h: T × X ⟶ T
  - H_i - chaining variables
- Padding block PB: 1000… || msg len
  - msg len (on 64 bits) complicates adversary's task
  - If no space for PB add another block

26

Merkle-Damgard collision resistance

- THEOREM. if compression function h is collision resistant (and message length is part of the input) then so is H.
  - Proof (by contradiction)
    - Collision on H ➔ collision on h. Q.E.D.
- Comment
  - To construct a CRHF, it *suffices* to construct a collision resistant compression function

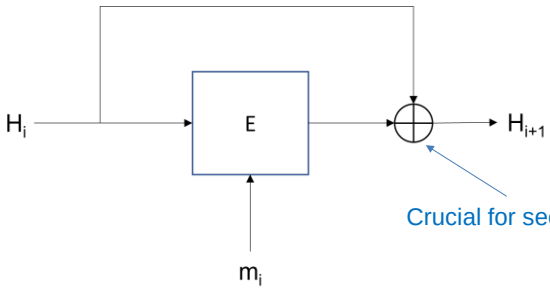
27

Hash functions from block ciphers

- Use block cipher chaining techniques
  - Matyas-Meyer-Oseas
  - Davies-Meyer
  - Miyaguchi-Preneel
  - Use block ciphers with 192/256 bit blocks
    - E.g. AES
- Cons
  - (digest size = block size) may be not enough for collision resistance
  - Possible solutions
    - Use block cipher with larger blocks (AES-192, AES-256)
    - Hirose scheme: use several instances of the block cipher

28

Davies-Meyer



- Finding a collision h(H, m) = h(H',m') requires $2^{m/2}$ evaluations of (E, D) ⇒ best possible!

29

Exercise

- Problem
  - If we remove the xor, the compression function is not collision resistant anymore.
  - Proof (by contradiction)
    - Remove the xor ➔ h(H, m) = E(m, H)
    - To construct a collision (H, m) and (H', m') is easy
      - Choose a random triple (H, m, m')
      - Determine H' such that E(m, H) = E(m', H') ➔ H' = D(m', E(m, H)

Q.E.D.

30

The MD4 family

Algorithm		Output [bit]	Input [bit]	No. of rounds	Collisions found
MD5		128	512	64	yes
SHA-1		160	512	80	yes
SHA-2	**SHA-224**	224	512	64	no
	SHA-256	256	512	64	no
	SHA-384	384	1024	80	no
	SHA-512	512	1024	80	no

MD5

- Developed in 1991
- 128-bit outuput lenght
- Collisions found in 2004, should be non longer used
  - Collision attack: $O(2^{24.1})$
  - Chosen-prefix collision attack: $O(2^{39})$

SHA-1

- Designed by NSA and standardised by NIST in 1995
- 160 bits output length
- Collision on SHA-1 in 2017, now deprecated
  - CWI – Google team
  - Forged PDF documents
  - Running time
    - Over 9+ quintillion SHA1 computations that took 6,500 years of CPU computation and 100 years of GPU computations however 10^5 times faster than black box attack
      - https://www.cwi.nl/news/2017/cwi-and-google-announce-first-collision-for-industry-security-standard-sha-1

Other hash functions

- SHA-2 (NIST 2002)
  - 256-bit, 384-bit or 512-bit output lenght
  - No known significant weaknesses but its structure is similar to SHA-1 and MD5
- SHA-3/Keccak
  - Result from public competition from 2008-2012
  - Very different design than SHA family
    - Requirement from NIST to defend from possible weakness in SHA family
  - Support 224, 256, 384, and 512-bit output lenght

Hash functions

USES OF HASH FUNCTIONS

36

Uses of hash functions

- Digital signatures
  - Requires strong collision resistance
- Password storage
  - Requires weak collision resistance
- Authentication of origin
  - Requires weak collision resistance
- Identification (one-time password)
  - Requires weak collision resistance and one-wayness

37

Hash Functions

AUTHENTICATION OF ORIGIN

38

Integrity vs authentication

- Message integrity
  - The property whereby data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source
- Message origin authentication
  - A type of authentication whereby a party is corroborated as the (original) source of specified data created at some time in the past
- Data origin authentication => data integrity

39

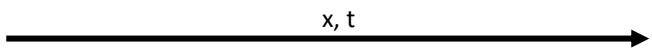
Use of hash functions for authentication

- The purpose of a hash functions, *in conjunction with other mechanisms* (authentic channel, encryption, digital signature), is to provide message integrity and authentication

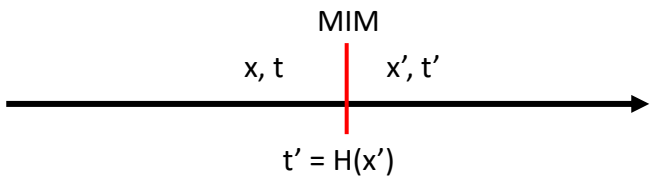
40

Authentic channel

- Alice Bob
  - Let t = H(x)



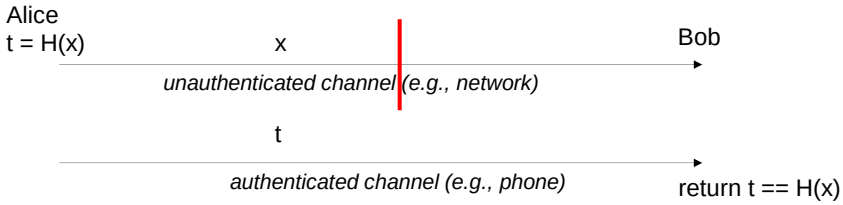
- MIM attack



41

Authentic channel

- Alice
  - Computes t = H(x)
  - Sends x to Bob through the network
  - Reads t to Bob over the phone
    - An additional channel considered authenticated by assumption



Hash functions with block ciphers

- $E_k(x||H(x))$ recommended
  - Confidentiality and integrity
  - As secure as E
  - H has weaker properties than digital signatures
- x, $E_k(H(x))$ not recommended
  - Prove that sender has seen H(x)
  - H must be collision resistant
  - Key k must be used only for this integrity function
- $E_k(x)$, H(x) not recommended
  - H(x) can be used to check guesses on x
  - H must be collision resistant

$G: 1^n \to (pubk, seck)$

$S(prvk, x) = \sigma$

$V(pubk, \sigma, x) = true/false$

$\forall x, (pubk, privk) \quad V(pubk, x, S(prvk, x)) = true$

$H(x) = h \qquad s = S(prvk, h||b)$

$(e, n) \qquad (d, n)$

$\sigma \equiv x^d \bmod n$

$V(prvk, \sigma, x) \equiv \quad x == \sigma^e \bmod n ?$

$\sigma \to \quad x = \sigma^e \bmod n$

$H: \{0,1\}^* \to \{0,1\}^n$

$x^d \bmod n \equiv (\sigma^e)^d \bmod n$

$\sigma_3 \equiv \sigma_1 \cdot \sigma_2 \bmod n$

$x_3 \equiv \sigma_3^e \equiv (\sigma_1 \cdot \sigma_2)^e \equiv \sigma_1^e \cdot \sigma_2^e \equiv x_1^e \cdot x_2^e \bmod n$

$\Sigma(G, S, V)$

- $t = H(t)$
- $s = t^d \bmod m$

$H : \{0,1\}^* \to \{0,1\}^n$

$\Sigma'(G, S', V')$

- $z < m$
- $y = z^e \bmod m$
- $x / y = H(x)$

$S' = S'(pwvk, x) = S(pwvk, H(x))$

$V' = V'(pubk, \sigma, x) = V(pubk, \sigma, H(x))$

- $x, s = S(pwvk, t)$ $\quad x_1, x_2 \;/\; H(x_2) = H(x_1)$
- $x_1, x_2 \;/\; H(x_2) = H(x_2)$

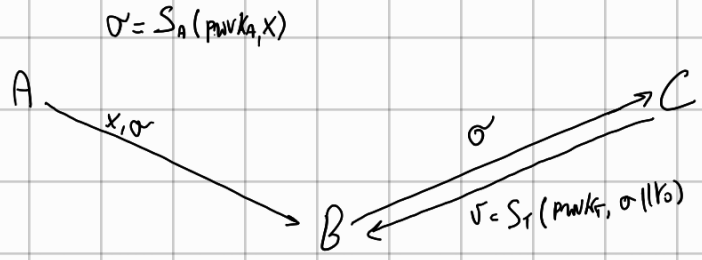
  (x_1, s) $\quad s = S(pwvk, H(x_1))$

G $\quad (pwvk, pubk)$

$\sigma = S(pwvk, x)$

$V(pubk, \sigma, x) = true/false$

- $\forall x, (pwvk, pubk)$ $\quad V(pubk, S(pwvk, x), x) = true$



$t = H(x) \qquad \tau = S(pwrk_1, t||r_0)$

• $(d, n) \quad (e, n)$

$\sigma \equiv x^d \bmod n$

$\sigma^e \bmod n = x$

• $\sigma \rightarrow \quad \sigma^e \bmod n \equiv x$

$x^d \equiv (\sigma^e)^d \bmod n \equiv \sigma$

• $\sigma_3 \equiv \sigma_1 \times \sigma_2$

$\downarrow x_3 \equiv x_1 \times x_3$

$x_3 \equiv \sigma_3^e \equiv (\sigma_1 \cdot \sigma_2)^e \equiv \sigma_1^e \cdot \sigma_2^e \equiv x_1 \cdot x_2 \bmod n$

$\Sigma(G, S, V)$

$H: \{0,1\}^* \to \{0,1\}^n$

$\Sigma'(G, S', V')$

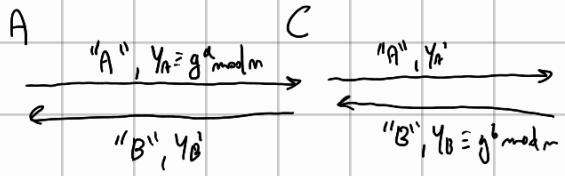
$$S'(x, pwvk) = S(H(x), pwvk)$$
$$V'(x, \sigma, pubk) = V(H(x), \sigma, pubk)$$

- $t = H(x)$ $\quad s = t^d \bmod n$ $\quad \cdot (d, n)$ $\cdot (e, n)$
- $z < n$

  $y \equiv z^e \bmod n$

  $x \,/\, H(x) = y$

- $\sigma = S(t, pwvk)$ $\quad t = H(x)$ $\quad \cdot x, \sigma$
- $x, x' \,/\, H(x) = H(x')$
- (x, s) $\quad s = g(x, pwvk)$



$|\mathbb{Z}_p^*| = p-1 = m$

$$Y_A' \equiv Y_A^{m/r} \equiv (g^{\frac{m}{r}})^a \bmod m$$
$$Y_B' \equiv (g^{m/r})^b \bmod m$$

A

B

- p, α
- $d \in \{2, \dots p-2\}$
- $\beta = \alpha^d \bmod m$

(p, α, β)

- $n \in \{2, \dots p-2\}$
- $k_E \equiv \alpha^n \bmod p$
- $k_M \equiv \beta^n \bmod p$
- $y \equiv x \cdot k_M \bmod p$

(k_E, y)

$k_M \equiv k_E^d \bmod p$

$x = y \cdot k_M^{-1} \bmod p$

$$x \equiv y \cdot k_M^{-1} \bmod p \equiv (x \cdot (\alpha^q)^n) \cdot ((\alpha^n)^d)^{-1} \bmod p \equiv x \cdot \alpha^{dn-nd} \equiv x \bmod p$$

- $(p, \alpha, \beta), (y, k_E)$ $k_E \equiv \alpha^n \bmod p$ $\beta \equiv \alpha^d \bmod p$ $y = x \cdot \beta^n \bmod p$
- $(y \cdot s, k_E)$ $x' \equiv x \cdot s \bmod p$

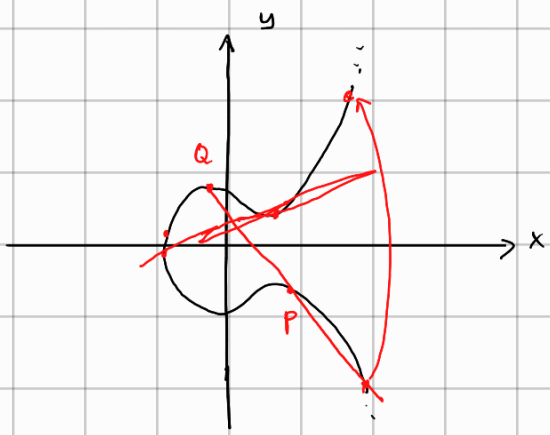
(y_1, k_E) (y_2, k_E)

$y_1 = x_1 k_M \bmod p \rightarrow k_M = y_1 x_1^{-1} \bmod p$

$x_2 = y_2 k_M^{-1} \bmod p$

$y^2 \equiv x^3 + ax + b \bmod p$

$4a^3 + 27b^2 \neq 0$



$P = (x_1, y_1)$

$Q = (x_2, y_2)$

$S = P + Q$

$\forall P \quad P + \mathcal{O} = P$

$-P : \quad P + (-P) = \mathcal{O}$

$a = \log_P A$

$b = \log_P B$

$P = (x_1, y_1) \qquad -P = (x_1, p - y_1)$

$E, T, P \qquad 1 \leq d \leq \#E$

- $P, C, d, P \rightarrow T_{AB} = a \cdot b \cdot P$

$T + T + \dots + T = dT = P$

- $P, P, b, C \qquad y^2 \equiv x^3 + cx + d \bmod p$

A

$a \in \{2, \dots, \#E - 1\}$

$A = a \cdot P$

$T_{AB} = a \cdot B$

B

$b \in \{2, \dots, \#E - 1\}$

$B = b \cdot P$

$T_{BA} = b \cdot A$

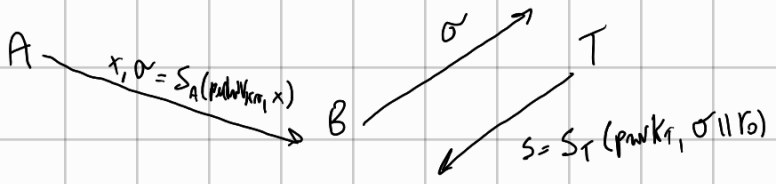
$a \cdot B = a \cdot (b \cdot P)$

G $(prvk, pubk)$

S $\sigma = S(x, prvk)$

V $V(x, \sigma, pubk)$

$\forall x, (prvk, pubk)$ $\quad V(x, pubk, S(prvk, x)) = true$



$T = H(x)$ $\quad s = S(prvk, T || r_0)$

$\sigma \equiv x^d \bmod n$

$x \equiv \sigma^e \bmod n$

$x^d \equiv (\sigma^e)^d \equiv \sigma^{ed} \bmod n$

$\sigma^e \bmod n \equiv x$

- $\sigma_3 \equiv \sigma_1 * \sigma_2$

  $x_3 = \sigma_3^e \equiv (\sigma_1 * \sigma_2)^e \equiv x_1^{de} \cdot x_2^{de} \bmod n$

$\Sigma(G, S, V)$

$H: \{0,1\}^* \to \{0,1\}^m$

$\Sigma'(G, S', V')$

$S'(x, prvk) = S(H(x), prvk)$

$V'(x, \sigma, pubk) = V(H(x), \sigma, pubk)$

- $t = H(x)$ $\quad s \equiv t^d \bmod n$
  - $z < n$ $\quad y \equiv z^e \bmod n$ $\quad$ • $x / H(x) = y$

A C B

$A \equiv \alpha^a \bmod p$ → ← $B \equiv \alpha^b \bmod p$

$m = |\mathbb{Z}_p^*| = p-1$

$A' \equiv A^{\frac{m}{K}} \equiv (\alpha^{\frac{m}{K}})^a \bmod p$

$B' \equiv (\alpha^{\frac{m}{K}})^b \bmod p$

$y \equiv x \cdot K_M \bmod p$

A B

- p, α
- $d \in \{2, \dots p-2\}$
- $\beta \equiv \alpha^d \bmod p$

(p, α, β) ←

- $i \in \{2, \dots p-2\}$
- $K_E \equiv \alpha^i \bmod p$
- $K_M \equiv \beta^i \bmod p$

$y \equiv x \cdot K_M \bmod p$

(y, K_E) →

$K_M \equiv K_E^d \bmod p$

$x \equiv y \cdot K_M^{-1} \bmod p$

- (p, α, β) , (y, K_E) $\quad y \equiv x \cdot \beta^i \bmod p$ $\quad K_E \equiv \alpha^i \bmod p$

- $K_E = \alpha^d \bmod p$
- $K_M = \beta^d \bmod p$

(y_1, K_E) , (y_2, K_E)

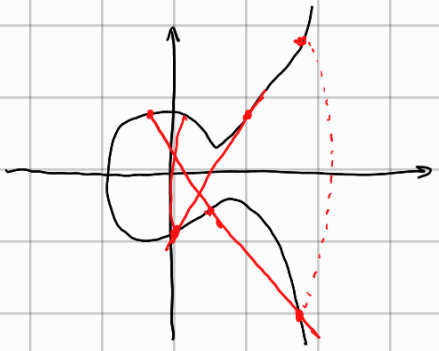
- $x_1 \equiv y_1 \cdot K_M^{-1} \bmod p$ $\quad x_2 \equiv y_2 \cdot K_M^{-1} \bmod p$

- $(y, K_E) \to (s \cdot y, K_E)$

$x' \equiv x \cdot s \bmod p$

(x,y) , $x, y \in \mathbb{Z}_p$ $\quad y^2 \equiv x^3 + ax + b \bmod p$

- $a^3 \cdot 4 + 27b^2 \neq 0$



$P = (x_1, y_1)$
$Q = (x_2, y_2)$
$S = P + Q$

$\forall P \quad P + \mathcal{O} = P$

$-P$ / $P + (-P) = \mathcal{O}$

$P = (x_1, y_1)$ $\quad -P = (x_1, p - y_1)$

E, P, T $\quad 1 \le d \le \#E$

$P + P + \dots + P = T$

d P

- $p, P, c, d \;/\; y^2 \equiv x^3 + cx + d \bmod p$

  - A
    $a \in \{2, \dots, \#E-1\}$
    $A = a \cdot P$
    $T_{AB} = a \cdot B$

  - B
    $b \in \{2, \dots, \#E-1\}$
    $B = b \cdot P$
    $T_{AB} = b \cdot A$

$X \equiv y \cdot k_M^{-1} \bmod p$

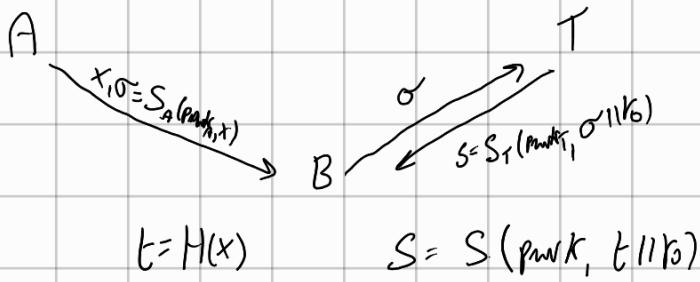
$X \equiv (x - (\alpha^d)^d) \cdot ((\alpha^d)^d)^{-1} \equiv x \cdot \alpha^{dd - dd} \equiv X \bmod p$

$a \cdot B = a \cdot (b \cdot P)$
$b \cdot (a \cdot P)$

- $p, c, d, P, A, B \qquad T_{AB} = a \cdot b \cdot P$
  - $a = \log_P A$
    $b = \log_P B$

- G $(pubk, privk)$
- S $S(privk, x) = \sigma$
- $\sqrt{}$ $\sqrt{}(pubk, \sigma, x) = T/F$

$\forall x, (pubk, privk) \qquad \sqrt{}(pubk, x, S(privk, x)) = True$



$t = H(x)$ $\qquad S = S(privk, t \| r_0)$

(e, m) (d, m)

- $s \equiv x^d \bmod m$
- $x \equiv s^e \bmod m$
- $\sigma \rightarrow x \equiv \sigma^e \bmod m$

  $x^d \equiv (\sigma^e)^d \bmod m$

- $\sigma_3 \equiv \sigma_1 \times \sigma_2$

  $x_3 \equiv \sigma_3^e \equiv (\sigma_1 \times \sigma_2)^e \equiv (x_1^d)^e \times (x_2^d)^e \bmod m \equiv x_1 \times x_2 \bmod m$

$\sum (G, S, V)$

$\sum' (G, S', V')$

$H : \{0,1\}^* \rightarrow \{0,1\}^n$

$S'(x, pubk) = S(H(x), pubk)$

$V'(x, \sigma, pubk) = V(H(x), \sigma, pubk)$

- (x, s)
- $x' / H(x') = H(x)$

- $H(x) = H(x')$

  (x, s)

- $s \equiv t^e \bmod m$

  $t = H(x)$

- $z < m$
- $y \equiv z^e \bmod m$
- $x / H(x) = y$

p, g

A — M — B

$a \to A = g^a \bmod p$ — A → — A' → — B' ← — B ← — $b \to B = g^b \bmod p$

$$A' \equiv A^{\frac{m}{K}} = \left(g^{\frac{m}{K}}\right)^a \bmod p$$

$$B' = B^{\frac{M}{K}} = \left(g^{\frac{m}{K}}\right)^b \bmod p$$

A

B

p, α

$d \in \{2, \dots p-2\}$

$B \equiv \alpha^d \bmod p$

(p, α, B) ←

- $N \in \{2, \dots, p-2\}$
- $K_E \equiv \alpha^N \bmod p$
- $K_M \equiv (B)^N \bmod p$
- $y \equiv x \cdot K_M \bmod p$ — (y, K_E) →

$K_M \equiv (K_E)^d \bmod p$

$x = K_M^{-1} \cdot y \bmod p$

$$x \equiv x \cdot (B)^N \cdot (K_E^d)^{-1} \equiv x \cdot (\alpha^d)^N \cdot ((\alpha^N)^d)^{-1} \equiv x \cdot \alpha^{dN - Nd}$$

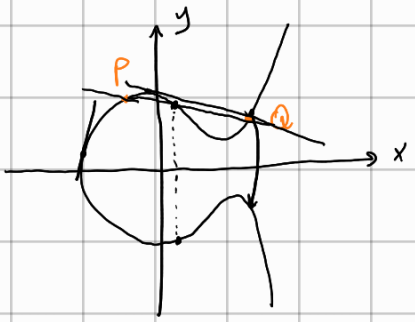
(p, α, B), (y, K_E) $\quad K_E \equiv (\alpha)^N \bmod p$

$B \equiv \alpha^d \bmod p$

(y_1, K_E) $\quad (y_2, K_E)$

$y_1 \equiv x_1 \cdot K_E \bmod p$ $\quad K_E = y_1 \cdot x_1^{-1} \bmod p$

- $\mathbb{Z}_p$, $p > 3$ $\quad y^2 \equiv x^3 + ax + b \bmod p$
  - $a^3 \cdot 4 + 27b^2 \neq 0$



$E, P \to T$

$1 \le d \le E$

$P + P + \dots + P = d \cdot P = T$

A

$a \in \{1, \dots, \#E\}$

$A = a \cdot P$

$T = a \cdot B$

$\hookrightarrow a \cdot (b \cdot P)$

B

$b \in \{1, \dots, \#E\}$

$B = b \cdot P$

$T = b \cdot A$

$\downarrow$

$b \cdot (a \cdot P)$

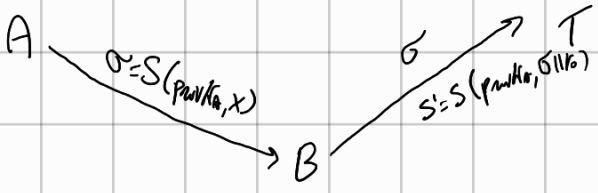
$(a, b, P, P, A, B) \qquad T = a \cdot B = b \cdot A$

(Gen, S, V)

$\sigma = S(privK, x)$

$V(\sigma, pubK, x)$

$\forall x, (pubK, privK) \quad V(x, pubK, S(privK, x)) = true$



$t = H(\sigma) \qquad \sigma = S(privK_T, t||r_0)$

A

(d, n) (e, n)

$t \equiv x^d \bmod n$ $x \equiv t^e \bmod n$

$(x^d) \equiv (t^e)^d \bmod n$

$\sigma_1 \equiv x_1^d \bmod n$

$\sigma_2 \equiv x_2^d \bmod n$

$\sigma \equiv \sigma_1 \cdot \sigma_2 \bmod n \quad (x_1 \cdot x_2) \bmod n$

$\sigma^e \equiv (\sigma_1 \cdot \sigma_2)^e \equiv \sigma_1^e \cdot \sigma_2^e \equiv x_1 \cdot x_2 \bmod n$

$\Sigma(G, S, V)$

$H: \{0,1\}^* \to \{0,1\}^n$

$\Sigma'(G, S', V')$ $\quad S'(x, pwd) = S(H(x), pwd)$

$V'(x, \sigma, pubk) = V(H(x), \sigma, pubk)$

- $y \equiv t^e \bmod n$
- $t = H(x) \quad \sigma = S(pwd, t)$

$A = (\alpha^a) \bmod p \qquad B = (\alpha^b) \bmod p$

$A' = (\alpha^a)^{\frac{M}{K}} \bmod p = (\alpha^{\frac{M}{K}})^a \bmod p$

$\uparrow B$

A

B

- α, $d \in \{2, \dots p-2\}$
- $\beta \equiv \alpha^d \bmod p$

(p, α, β)

- $s \in \{2, \dots p-2\}$
- $K_E \equiv \alpha^s \bmod p$
- $K_M \equiv (\beta)^s \bmod p$
- $y \equiv x \cdot K_M \bmod p$

(y, K_E)

- $K_M \equiv (K_E)^d \bmod p$
- $x \equiv y \cdot K_M^{-1} \bmod p$

$$x \equiv y \cdot K_M^{-1} \equiv x \cdot (\alpha^d)^s \cdot ((\alpha^s)^d)^{-1} \equiv x \cdot \alpha^{d \cdot s - s d} \bmod p$$

$(K_E, y \cdot s) \rightarrow x' \equiv y \cdot s \cdot K_M^{-1} \bmod p$

$(K_E, y_1) \quad (K_E, y_2)$

$y_1 \equiv x_1 K_M \bmod p$

$x_2 \equiv y_2 K_M^{-1} \bmod p$

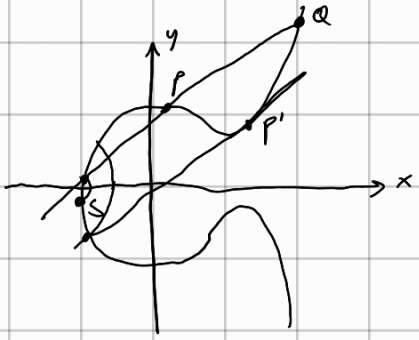
(p, α, β) , $(y, K_E) \quad K_E \equiv \alpha^s \bmod p$

$y = x \cdot K_M \bmod p$

$p > 3$

- $\mathbb{Z}_p \quad (x, y) \mid x, y \in \mathbb{Z}_p \quad y^2 \equiv x^3 + ax + b \bmod p$
  - $a^3 \cdot 4 + b^2 \cdot 27 \neq 0$

$P(x_1, y_1) \qquad Q(x_2, y_2)$



$P + \mathcal{O} = P \qquad P(x, y) \quad -P(x, p-y)$

$P + (-P) = \mathcal{O}$

- E, P, T

$1 \leq X \leq \#E$

$P + P + \ldots + P = T = P \cdot X$

$P, a, b \qquad y^2 \equiv x^3 + ax + b \bmod p$

A

$a' \in \{2, \ldots \#E\}$

$Y_A = a' \cdot P$

$K_{AB} = a' Y_B$

B

$b' \in \{2, \ldots \#E\}$

$Y_B = b' \cdot P$

$K_{BB} = b' Y_A$

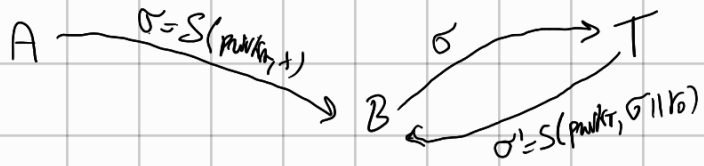
$K_{AB} = a' \cdot (b' \cdot P) = b' \cdot (a' \cdot P)$

- $p, a, b, Y_A, Y_B \longrightarrow K = a' \cdot b' \cdot P$

$\forall x, \ (pubK, privK)$

$V(pubK, x, S(privK, x)) = \text{true}$ $\quad S(privK, x) = \sigma$

$V(pubK, \sigma, x)$



$t = H(x)$ $\quad \sigma = S(pwrk_T, t \| r_0)$

(e, n) $\quad (d, n)$

- $t \equiv x^d \bmod n$
- $x^e \bmod n \equiv t$

- $\sigma \rightarrow \quad \sigma^e \bmod n \equiv x$

$\sigma_1 \equiv x_1 \bmod n$ $\quad \sigma_3 \equiv \sigma_1 \times \sigma_2 \bmod n$

$\sigma_2 \equiv x_2 \bmod n$ $\quad \sigma_3^e \equiv (\sigma_1 \cdot \sigma_2)^e \bmod n \equiv x_1^{d \cdot e} \cdot x_2^{d \cdot e} \bmod n$

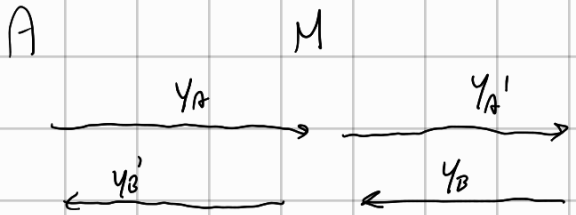
$H : \{0,1\}^* \rightarrow \{0,1\}^n$

$\Sigma'(Gen, S', V') \rightarrow \quad S'(pwrk, x) = S(pwrk, H(x))$

$V'(pubk, \sigma, x) = V(pubk, \sigma, H(x))$

- $t = H(x)$ $\quad s = S(pwrk, t)$

- $y \equiv z^e \bmod n$
  ↳ $x \mid H(x) = y$



$$y_A' \equiv (y_A)^{\frac{m}{k}} \bmod p \equiv (g^{\alpha})^{\frac{m}{k}} \bmod p \equiv (g^{\frac{m}{k}})^{\alpha} \bmod p$$

β

A B

$d \in \{2, \dots, p-2\}$

$B \equiv \alpha^d \bmod p$

(p, α, B)

- $s \in \{2, \dots p-2\}$

$K_E \equiv \alpha^s \bmod p$

$K_M \equiv (B)^s \bmod p$

$y \equiv x \cdot K_M \bmod p$

(y, K_E)

$K_M \equiv K_E^d \bmod p$

$x \equiv y \cdot K_M^{-1} \bmod p$

$$x \equiv (x \cdot K_M) \cdot (K_E^d)^{-1} \equiv (x \cdot (\alpha^d)^s) \cdot ((\alpha^s)^d)^{-1} \equiv x \cdot \alpha^{sd - ds} \equiv x \bmod p$$

- (y_1, K_E) (y_2, K_E)

$x_1, y_1 \rightarrow$ $y_1 \equiv x_1 \cdot K_M \bmod p$ $x_2 \equiv y_2 \cdot K_M^{-1} \bmod p$

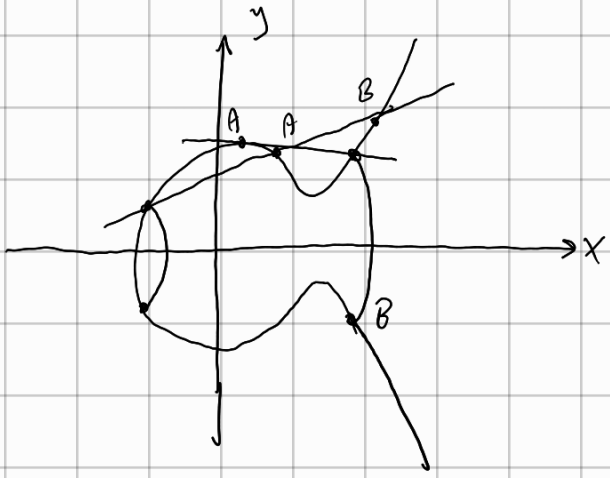
(α, β, p) (K_E, y)

$\beta \equiv \alpha^d \bmod p$ $y \equiv x \cdot K_M \bmod p$

$\mathbb{Z}_p$

$(x,y) / x,y \in \mathbb{Z}_p$ $\quad y^2 \equiv x^3 + ax + b \bmod p$

$4a^3 + 27b^2 \neq 0$



$A(x_1, y_1)$

$B(x_2, y_2)$

$(-P) + P = \mathcal{O}$

E, P, T

$1 \leq d \leq \#E /$

$T = P + P_{+} \ldots + P = dP$

$p, a, b \rightarrow \quad y^2 \equiv x^3 + ax + b \bmod p$

A

$a' \in \{2, \ldots, \#E - 1\}$

$A = a'T$

$K = a'B = a' \cdot (b'T) = b' \cdot (a' \cdot T)$

B

$b' \in \{2, \ldots, \#E - 1\}$

$B = b'T$

$K = b'A$

$S(pubk, x) = \sigma \qquad V(pubk, \sigma, x) = T/F$

A $\xrightarrow{x, \sigma}$ $\sigma = S(pubk_A, x)$ B

B $\xrightarrow{\sigma}$ T

$\sigma \stackrel{?}{=} S(pubk_T, G \| r_0)$

$H(x) = t \qquad \sigma = S(pubk_T, t \| r_0)$

- RSA
  - $(e, m) \quad (d, m)$
  - $t \equiv x^d \bmod m$
  - $t^e \bmod m \equiv x$

    - $\sigma \rightarrow \sigma^e \bmod m \equiv x$
    - $\sigma_1 \equiv x_1^d \bmod m \qquad \sigma_2 \equiv x_2^d \bmod m$
      $\sigma \equiv \sigma_1 \cdot \sigma_2 \bmod m \qquad \sigma^e \equiv \sigma_1^e \cdot \sigma_2^e \bmod m \equiv x_1 \cdot x_2 \bmod m$

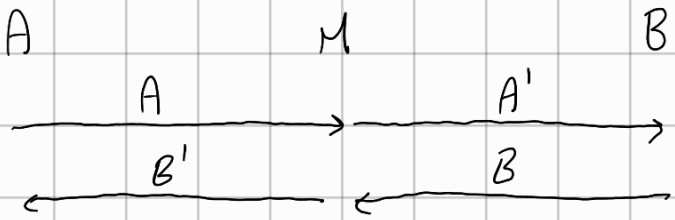
(G, S, V)

$H: \{0,1\}^* \rightarrow \{0,1\}^n$

$\Sigma' = (G, S', V')$

$S' = S(H(x), \text{pwk})$
$V'(x, \sigma, \text{pubk}) = V(H(x), \sigma, \text{pubk})$

$t = H(x) \qquad s \equiv t^d \bmod m$
$z \rightarrow y \equiv z^e \bmod m$
$x / H(x) = y$



$$A \to A' = A^{\frac{m}{k}} \equiv (g^a)^{\frac{m}{k}} \bmod p \equiv (g^{\frac{m}{k}})^a \bmod p$$
$$B' \equiv (g^{\frac{m}{k}})^b \bmod p$$

A

B
- $d \in [2, p-2]$
- $\beta \equiv \alpha^d \bmod p$

(β, α, p)

- $N \in [2, p-2]$
- $k_E \equiv \alpha^N \bmod p$
- $k_M \equiv (\beta)^N \bmod p$
- $y \equiv X \cdot k_M \bmod p$ $\xrightarrow{(y, k_E)}$ $k_M \equiv k_E^d \bmod p$, $X \equiv y \cdot k_M^{-1} \bmod p$

$$X \equiv y \cdot k_M^{-1} \equiv (x \cdot (\alpha^d)^N) \cdot ((\alpha^N)^d)^{-1} \equiv x \cdot \alpha^{dN - Nd} \equiv X$$

(y_1, k_E) (y_2, k_E) $(y \cdot S, k_E)$

$y_1 \equiv x_1 \cdot k_M \bmod p$ $x_2 \equiv y_2 \cdot k_M^{-1} \bmod p$

(β, α, p) (y, k_E) $y \equiv x \cdot k_E^d \bmod p$ $x' \equiv y \cdot S k_M^{-1} \bmod p \equiv x \cdot S \bmod p$

$B \equiv \alpha^d \bmod p$

$p > 3$ $\mathbb{Z}_p$

↳ $(x,y) / x, y \in \mathbb{Z}_p$

$y^2 \equiv x^3 + ax + b \bmod p$

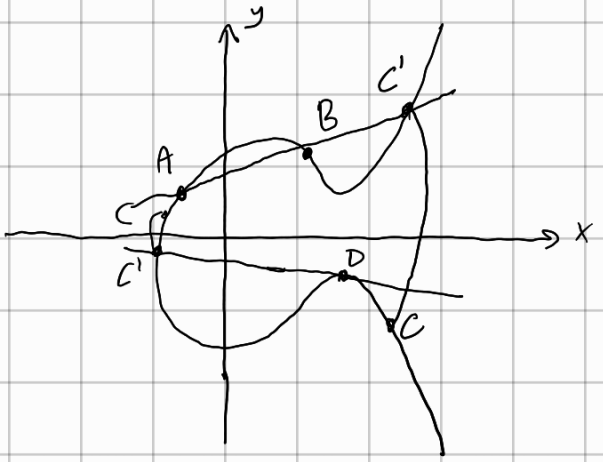
$4a^3 + 27b^2 \neq 0 \bmod p$

$A(x_1, y_1)$ $B(x_2, y_2)$

$C(x_3, y_3)$

$P + \vartheta = P$

$-P \;/\; P + (-P) = \vartheta$



- $\#E$

  P, T $\quad 1 \leq d \leq \#E \;/\; P + P + P + \dots + P = dT$

- a, b, p : $y^2 \equiv x^3 + ax + b \bmod p$
- P

A

$a' \in \{2, \dots \#E - 1\}$

$A = a'P$

$K = a'B$

B

$b' \in \{2, \dots, \#E - 1\}$

$B = b'P$

$K = b'A$

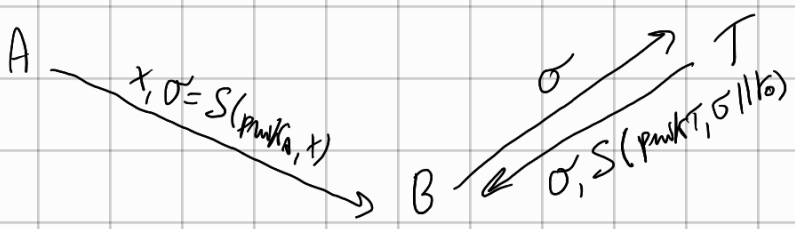
$a'B = b'A = a' \cdot b' P$

(a, b, p, P, A, B) $\quad K = a' \cdot b' \cdot P$ $\quad a' \cdot (b' \cdot P) = b' \cdot (a' \cdot P)$

$\sigma = S(pwvk, x)$

$V(pubk, \sigma, x) = \begin{matrix} true \\ false \end{matrix}$

$\forall x, (pubk, pwvk) \quad V(pubk, x, S(pwvk, x)) = true$



$t = H(x) \qquad \sigma = S(pwvk_T, t || r_0)$

- $(d, n) \qquad (e, n)$

- $\sigma \equiv x^d \bmod n$
- $x \equiv \sigma^e \bmod n$

(G, S, V)

$H: \{0,1\}^* \to \{0,1\}^m$

$\sigma_1 \equiv x_1^d \bmod n \qquad \sigma_2 \equiv x_2^d \bmod n$

$\sigma_3 \equiv \sigma_1 \cdot \sigma_2$

$(\sigma_3)^e \equiv \sigma_1^e \cdot \sigma_2^e \equiv x_1 \cdot x_2 \bmod n$

$\Sigma'(G, S', V')$:

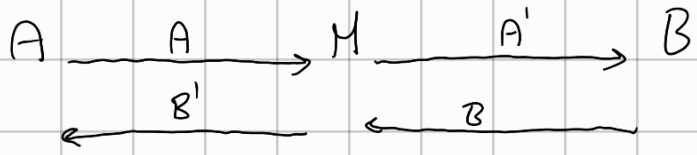
$S'(x, pwvk) = S(H(x), pwvk)$

$V'(x, pubk, t) = V(H(x), pubk, t)$

$t = H(x) \qquad s \equiv t^d \bmod n$

- $z \to y \equiv z^e \bmod n$

  $x \,/\, H(x) = y$



$|\mathbb{Z}_p^*| = n$

$A \equiv \alpha^a \bmod p$

$A' \equiv (\alpha^a)^{\frac{n}{r}} \equiv (\alpha^{\frac{n}{r}})^a \bmod p \equiv \beta^a \bmod p$

$B' \equiv \beta^b \bmod p$

A

B

$\alpha \in \mathbb{Z}_p^*$

$d \in [2, p-2]$

$\beta \equiv \alpha^d \bmod p$

(p, α, β) ←

- $s \in [2, p-2]$
- $K_E \equiv \alpha^s \bmod p$
- $K_M \equiv \beta^s \bmod p$
- $y \equiv x \cdot K_M \bmod p$ → (K_E, y)

$K_M \equiv K_E^d \bmod p$

$x \equiv y \cdot K_M^{-1} \bmod p$

(y_1, K_E) , (y_2, K_E) $\quad y_1 \cdot x_1^{-1} \equiv K_M \quad x_2 \equiv y_2 \cdot K_M^{-1} \bmod p$

$(y \cdot S, K_E)$ $\quad x' \equiv y' \cdot K_M^{-1} \bmod p \equiv x \cdot S$

$x \equiv y \cdot K_M \equiv (x \cdot (\alpha^d)^r) \cdot (\alpha^{rd})^{-1} \equiv x \cdot \alpha^{dr - rd} \equiv x \bmod p$

(p, α, B) $\quad (y, K_E)$

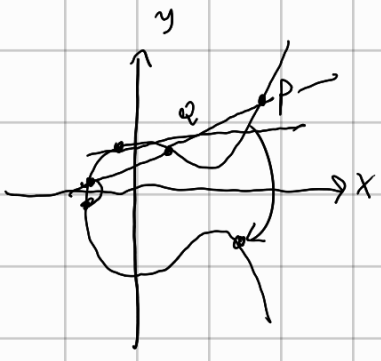
$B \equiv \alpha^d \bmod p$ $\quad y \equiv x \cdot \alpha^r \bmod p$

$\mathbb{Z}_p$

$(x, y) \in \mathbb{Z}_p$

$y^2 \equiv x^3 + ax + b \bmod p$

$4 \cdot a^3 + 27 b^2 \neq 0 \bmod p$



$P(x_1, y_1)$ $\quad Q(x_2, y_2)$

R

$\forall P \quad P + \mathcal{O} = P$

$P + (-P) = \mathcal{O}$

- $E, P, T \in E$

$1 \leq d \leq \#E$

$P + P + \ldots + P = d \cdot P = T$

$a, b, P \qquad y^2 \equiv x^3 + ax + b \bmod p$

A	B
$a' \in \{2, \dots, \#E-2\}$	$b' \in \{2, \dots, \#E-2\}$
$A = a' \cdot P$	$B = b' \cdot P$
$K_{AB} = a' \cdot B$	$K_{AB} = b' \cdot A$

$$K_{AB} = a' \cdot B = a' \cdot (b' \cdot P) = b' \cdot (a' \cdot P)$$

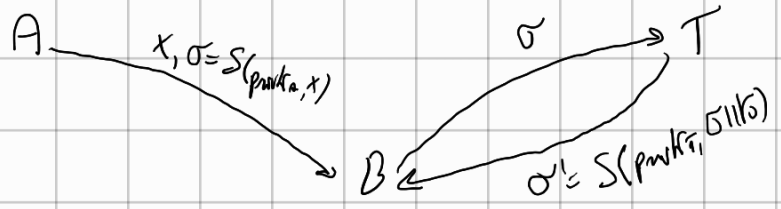
$a, b, P, A, B \qquad K = a' \cdot b' \cdot P$

$$a' = \log_P A$$
$$b' = \log_P B$$

$S(prvK, x) = \sigma$

$V(pubK, x, \sigma) = \begin{matrix} True \\ False \end{matrix}$

$\forall x, (pubK, prvK) \quad V(pubK, x, S(prvK, x)) = True$



$t = H(x) \qquad \sigma = S(prvK_T, t||r_B)$

$(e, n) \qquad (d, n)$

- $\sigma \equiv x^d \bmod n$
- $x \equiv \sigma^e \bmod n$

- $\sigma^e \equiv x$

$$x^d \equiv (\sigma^e)^d \bmod n \equiv \sigma$$

$\sigma_1 \equiv x_1^d \bmod n \qquad \sigma_2 \equiv x_2^d \bmod n$

$\sigma \equiv \sigma_1 \cdot \sigma_2 \bmod n$

$\sigma^e \equiv (\sigma_1 \cdot \sigma_2)^e \equiv x_1 \cdot x_2 \bmod n$

$\Sigma = (G, S, V)$

$H: \{0,1\}^* \to \{0,1\}^n$

$\Sigma' = (G, S', V')$

$S'(pwd_k, x) = S(pwd_k, H(x))$

$V'(pub_k, x, \sigma) = V(pub_k, H(x), \sigma)$

(x, σ) $t = H(x)$ $\sigma \equiv t^d \bmod n$

$x' / H(x') = H(x)$ $y \equiv \sigma^e \bmod n$