Cursus Cryptografie

PUBLICKEY

19-02-2016

Onderwerpen

- Principe
- Getaltheorie
- Priemgetallen
- Diffie-Hellman
- RSA
- ElGamal
- Elliptische krommen
- Merkle-Hellman knapzak

Principe

Klassiek = symmetrisch cryptosysteem

PublicKey = asymmetrisch cryptosysteem

Vindt functies waarmee:

- vercijfering *eenvoudig*
- ongewenste ontcijfering *ondoenlijk*
- afleiden geheime uit openbare sleutel *ondoenlijk*

Valluik

one way functie

eenvoudig: $y = f(x)$ onuitvoerbaar: $x = f^{-1}(y)$

trapdoor one way functie

onuitvoerbaar: $x = f^{-1}(y)$ eenvoudig: $x = f^{-1}(y,z)$

Maatstaf algoritmische complexiteit

- *eenvoudig* = polynomiaal $O(n^c)$
- *ondoenlijk* = exponentieel $O(c^n)$
- *brute force* = $O(2^n)$

Leverancier = getaltheorie

- discrete logaritme
- factorisatie

Getaltheorie

verzameling gehele getallen modulo n heet $\mathbb{Z}_n$

$$x \in \mathbb{Z} \to x \bmod n \in \mathbb{Z}_n \qquad \mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

weglaten getallen gemeenschappelijke factor met n levert $\mathbb{Z}_n^*$

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : x > 0 \wedge \text{ggd}(x, n) = 1\} \qquad \mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

een primitief element genereert $\mathbb{Z}_n^*$

$$\{x^0, x^1, x^2, \ldots\} = \mathbb{Z}_n^*$$

$$3, 7 \to \{1, 3, 7, 9\} = \mathbb{Z}_{10}^*$$

$$1 \to \{1\} \neq \mathbb{Z}_{10}^*$$

$$9 \to \{1, 9\} \neq \mathbb{Z}_{10}^*$$

Galois Field

puntjes op de i zoals
mits ggd(a,n)=1
maar met *n* is priem OK

Evariste Galois
1811–1832

Voor $\mathbb{Z}_n^*$ *gelden de volgende rekenregels*

1. $\forall x, y\colon\ a * x \equiv a * y \bmod n$ iff $x \equiv y \bmod n$
2. $a * \mathbb{Z}_n^* = \{a * x \bmod n\colon\ x \in \mathbb{Z}_n^*\} = \mathbb{Z}_n^*$
3. $\exists b \in \mathbb{Z}_n^*\colon\ a * b \equiv 1 \bmod n$

dan is $\mathbb{Z}_n^*$ *een Abelse groep onder vermenigvuldiging modulo n*

Gevolg: in $\mathbb{Z}_n^*$ kan correct gerekend worden

In publickey toepassing met p priemgetal en toevoeging nul

$\mathbb{Z}_p^* + \{0\} = \{0, 1, 2, \ldots, p-1\}$ *is Galois Field GF(p)*

Euler totiënt functie

Leonhard Euler 1707–1783

Euler totiënt functie $\phi(n)$

$$\phi(n) = \#i \text{ met } \gcd(i,n) = 1 \text{ voor } i = 1, 2, \ldots, n-1$$

$$\phi(p) = (p-1) \text{ voor } p \text{ priem}$$

$$\phi(p \cdot q) = (p-1)(q-1) \text{ voor } p, q \text{ priem}$$

Stelling van Euler

$$\gcd(p,n) = 1 \rightarrow p^{\phi(n)} \equiv 1 \bmod n$$

Kwadratische rest

Kwadratische rest $x \bmod p$ *als*

$$\exists y \in \mathbb{Z}_p^* \colon\ y^2 \equiv x \bmod p \rightarrow x \in \mathbb{Q}_p$$

Legendre symbool

$$L(a,p) = \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ +1 & \text{if } a \in \mathbb{Q}_p \\ -1 & \text{if } a \not\in \mathbb{Q}_p \end{cases}$$

Jacobi symbool

$$J(a,n) = \left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \ldots \quad n = p_1^{e_1} p_2^{e_2} \ldots$$

Priemgetallen

Gauss (1777–1855)

- aantal priemgetallen [2…*x*] ≈ π(*x*) = (*x* : *ln x*)
- met 100 cijfers = π(100) - π(99) ≈ 4.10^{97}
- *gemiddelde* afstand priemgetallen ≈ *ln x*
  voor 100 cijfers ±230, 150 cijfers ±345

priemgetallen niet alle evenwaardig: sterk priemgetal nodig

1. *p* - 1 heeft grote priemfactor *a*
2. *p* +1 heeft grote priemfactor *b*
3. *a* - 1 heeft grote priemfactor *c*

voor RSA *n* = 1024 bits → *p*,*q* ±150 cijfers

Priemtesten

- deterministisch
  Mersenne-priemgetallen speciale methode
  Agrawal-Kayal-Saxena-algoritme
- probabilistisch
  - Solovay-Strassen
    Euler getuige a voor *n niet priem*:
    $ggd(a,n) > 1$ en/of $J(a,n) \neq a^{(n-1)/2} \bmod n$
    Euler leugenaar a voor *n niet priem*:
    $ggd(a,n) = 1$ én $J(a,n) = a^{(n-1)/2} \bmod n$
    leugenaar heeft 50% kans → na 20 *a*'s < 0.0001%
  - Miller-Rabin
    sterke getuige of *sterke leugenaar* met 25% kans
- voor algoritmen: zie syllabus

Diffie-Hellman 1976

systeem voor sleuteluitwisseling

parameters

- *openbare systeeminformatie*
  GF(p) met *p* priem
  primitief element $a \in GF(p)$
- *geheime deelnemerinformatie*
  deelnemer *i* een $x_i \in GF(p)$
- *openbare deelnemerinformatie*
  $y_i = a^{x_i} \bmod p$

uitvoering

- deelnemer *i*
  $K_{ij} = a^{(x_i x_j)} = (a^{x_j})^{x_i} = y_j^{x_i}$
- deelnemer *j*
  $K_{ij} = a^{(x_i x_j)} = (a^{x_i})^{x_j} = y_i^{x_j}$

veiligheid

- $y_i = a^{x_i} \bmod p$ eenvoudig
- $x_i = \log_a y_i$ ondoenlijk

RSA 1978

Rivest Shamir Adleman

parameters

- *geheime systeeminformatie*
  priemgetallen p en q
  getal d met ggd(d, $\phi(n)$) = 1
- *openbare systeeminformatie*
  product $n = p \,.\, q$
  getal e met $ed = 1 \bmod \phi(n)$
- authentiseren omdat
  $M = D(E(M)) = E(D(M))$

uitvoering

- *verzender* bericht
  $C = E(M) = M^e \bmod n$
- *ontvanger* bericht
  $M = D(C) = C^d \bmod n$

veiligheid

- p, q groot → $n \geq 300$ cijfers
- factoriseren p en q uit n
  → exponentieel in n
- p, q, d, e zorgvuldig te kiezen

Werking van RSA

$$D(E(M)) = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n$$

$$ed \equiv 1 \bmod \phi(n) \rightarrow ed = k.\phi(n) + 1$$

$$\begin{aligned} M^{ed} \bmod n &= M^{k.\phi(n)+1} \bmod n \\ &= M.M^{k.\phi(n)} \bmod n \\ &= M.(M^{\phi(n)} \bmod n)^k \bmod n \end{aligned}$$

$$M^{\phi(n)} \equiv 1 \bmod n \text{ (Euler)} \rightarrow (M^{\phi(n)} \bmod n)^k = 1^k \bmod n = 1$$

$$M^{ed} \bmod n = M.1 \bmod n = M$$

Voorbeeld RSA

- Kies RSA parameters
  1. $p = 47$ en $q = 59 \rightarrow n = 2773$
  2. $\phi(n) = 46.58 = 2668$
  3. kies $d = 157$ en ggd-berekening met 2668,157 $\rightarrow$ $e = 17$
     met $ed = 17.157 = 2669 = 1 \bmod 2668$
- Codeerschema spatie = 00, A = 01, B = 02, …
- Vercijfering

```
    I T  S    A L  L    G R  E E  K    T O    M  E
M: 0920 1900 0112 1200 0718 0505 1100 2015 0013 0500
C: 0948 2342 1084 1444 2663 2390 0778 0774 0219 1655
```

- $0920^{17} = 0920^{10001} = 0948 \leftrightarrow 0948 = 0920$

Factoriseren

# cijfers	schatting 1985	realisering
100	1 jaar	
125	100 jaar	1994: RSA-129
150	10.000 jaar	1999: RSA-155
175	700.000 jaar	2003: RSA-176
200	30 miljoen jaar	2005: RSA-200
225	1 miljard jaar	2009: RSA-232
250	60 miljard jaar	

Zwakke plekken RSA

- FOUT gemeenschappelijke priemfactor $n_i = p \cdot q_i$
- FOUT meerdere e,*d* bij één enkele $n = p \cdot q$
- identieke berichten, verschillende *n* maar dezelfde e dan soms $Z_n \rightarrow Z$ reductie mogelijk
- lage exponent e en deels bekende klaartekst, bijvoorbeeld padding 64 bits sleutel → 1024 bits
- lage geheime exponent *d* gekoppeld met $|p - q|$ kan via kettingbreukontwikkeling van e/*n* de *d* opleveren

ElGamal 1984

parameters

- *openbare systeeminformatie*
  p priem → Z_p, $a \in Z_p$
- *geheime deelnemerinformatie*
  encryptie exponent s
- *openbare deelnemerinformatie*
  getal $b = a^s \bmod p$
- *geheime berichtsleutel*
  extra sleutel 0<k<p-1 *per bericht*

veiligheid

- discrete logaritme ondoenlijk
  $s = \log_a b \bmod p$

uitvoering

- verzender
  $C = (c_1,c_2) = (M.b^k,a^k)$
- ontvanger
  $M = D(c_1,c_2) = c_1c_2^{-s}$
  $= (M.b^k)(a^k)^{-s} = M.b^k.(a^s)^{-k}$
  $= M.b^kb^{-k} \bmod p = M$

valkuil

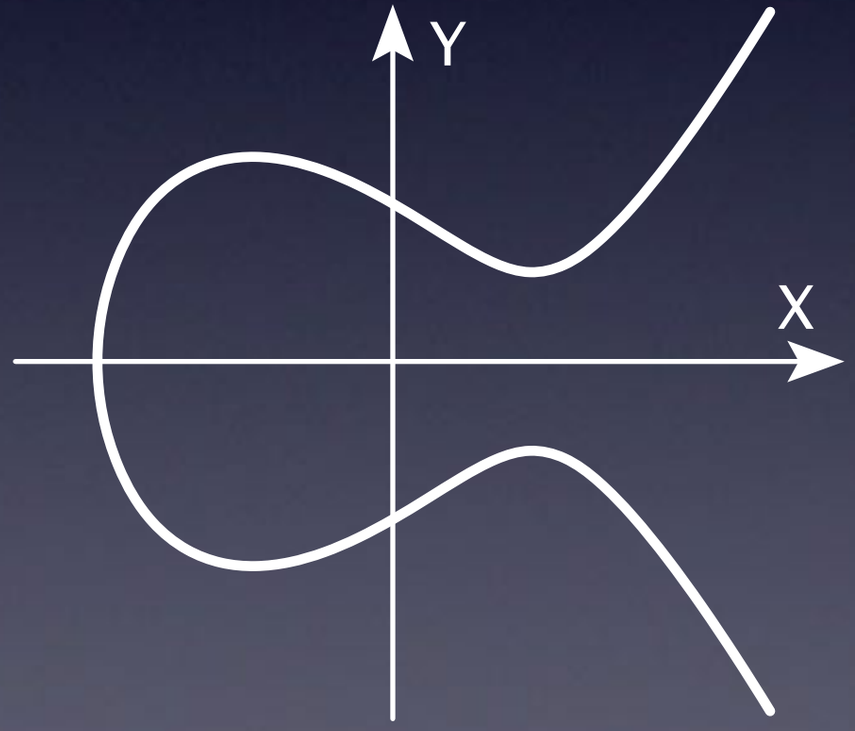
- $C = E(M,k), C' = E(M',k)$
- $M.c_1^{-1}c_1' =$
  $M.(M^{-1}b^{-k})(M'b^k)$
  $M.M^{-1}.M' = M'$

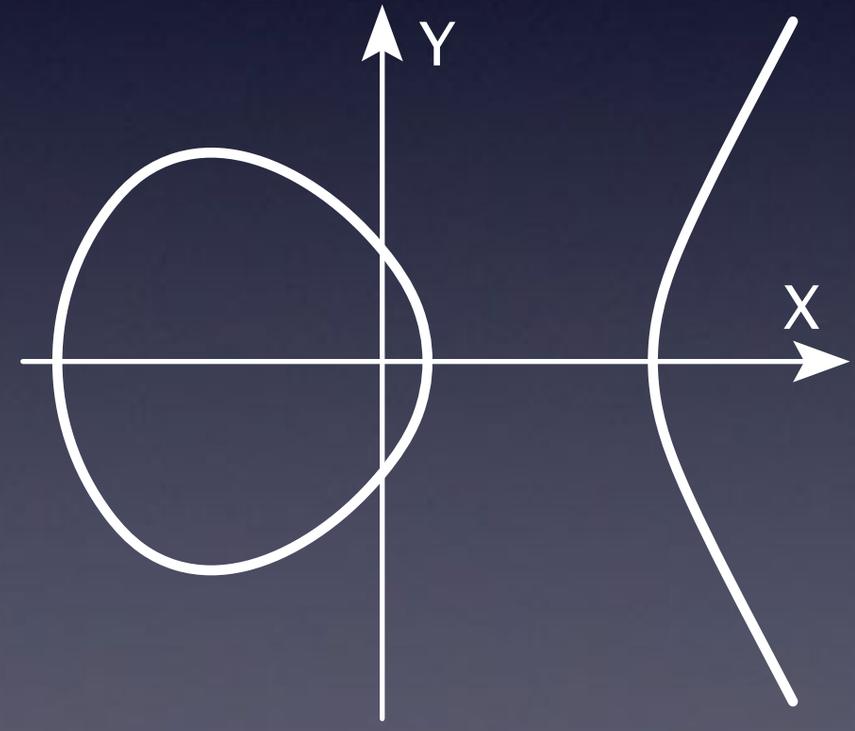
Elliptische krommen

$y^2 = x^3 + ax + b$

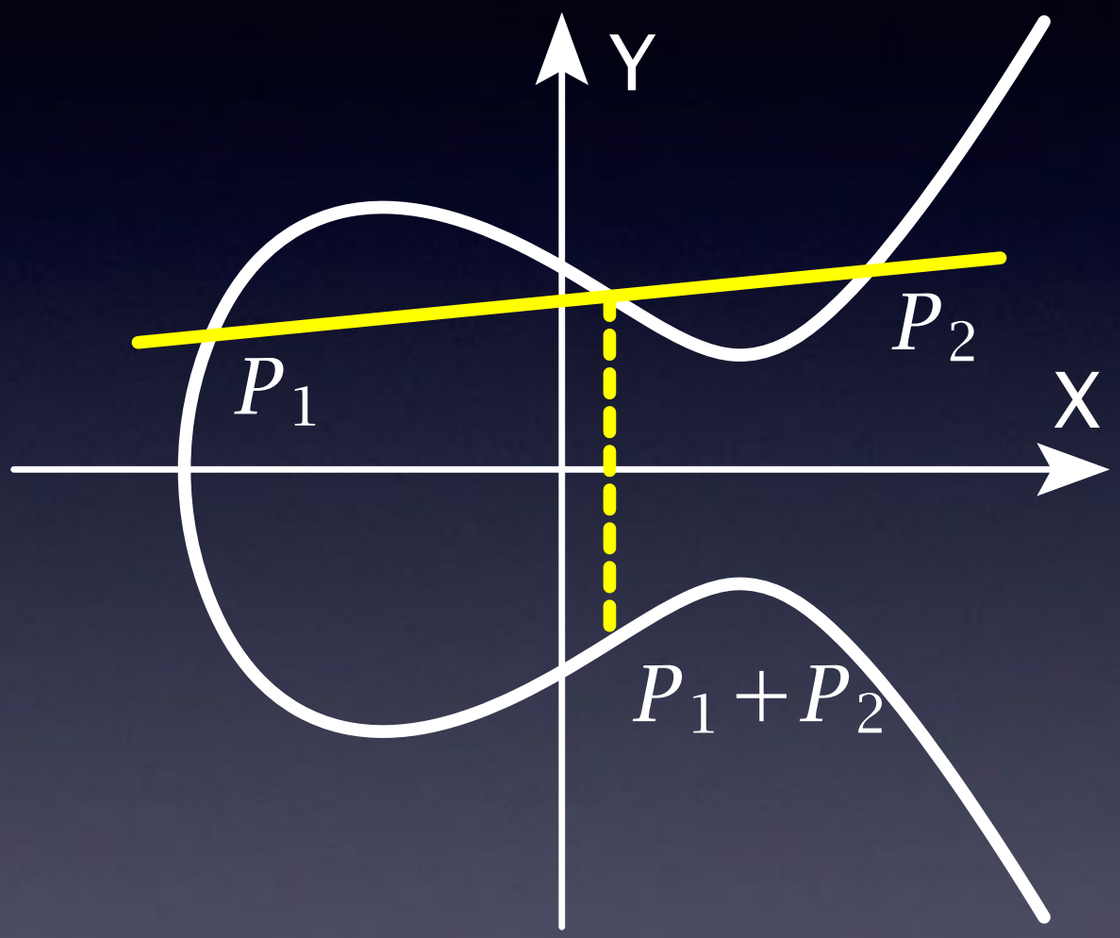
kies een verzameling punten op de curve

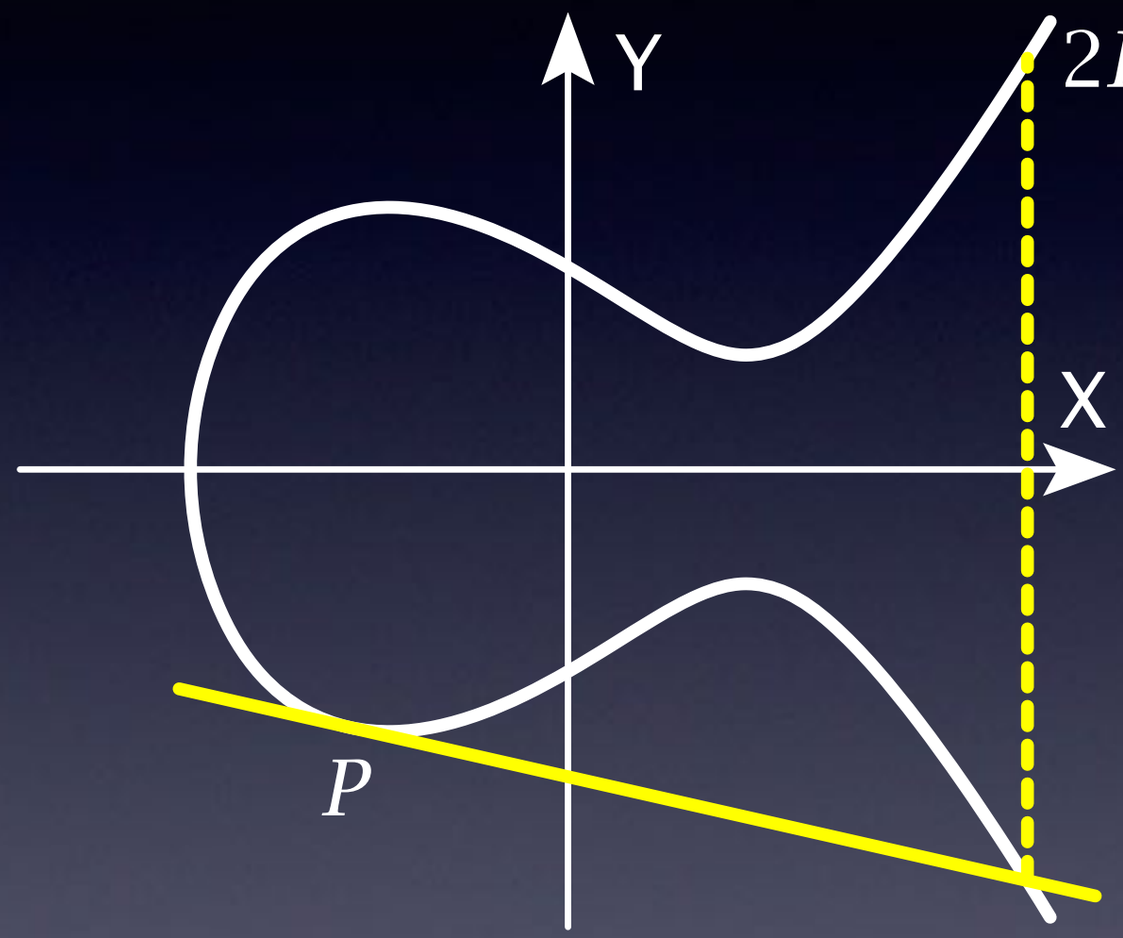
oorsprong O wordt in het oneindige genomen





Elliptic Curve Cryptografie





$$P_1 + P_2 = (x_1,y_1) + (x_2,y_2) = (\lambda^2\text{-}x_1\text{-}x_2,\ \lambda x_1\text{-}\lambda x_s\text{-}y_1)$$

Merkle-Hellman

parameters

- *geheime systeeminformatie*
  knapzakvector $a = (a_1,a_2,\ldots)$
  superstijgend $a_i > a_1+\ldots+a_{i-1}$
  $w,m > a_1+\ldots+a_n$ $ggd(w,m)=1$
- *openbare systeeminformatie*
  $b = (b_1,b_2,\ldots)$ permuteer b
  $b_i = w.a_i \bmod m$
- voorbeeld: zie syllabus

veiligheid

- drijfzand want complexiteit:
  superstijgend < NP-compleet

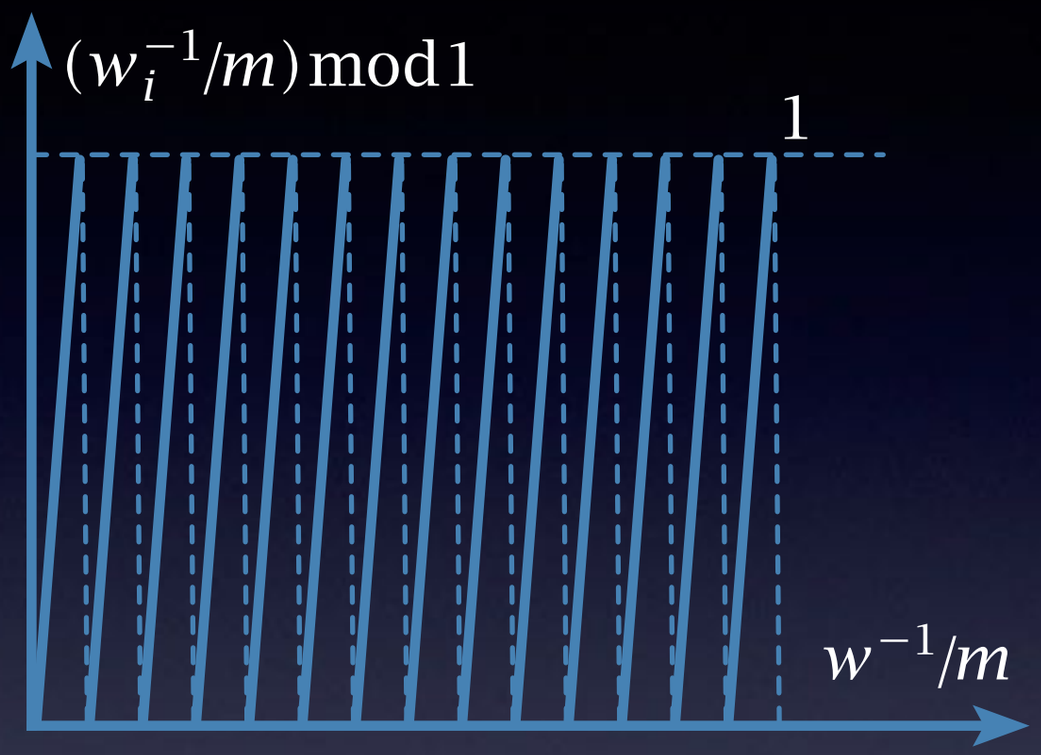
uitvoering

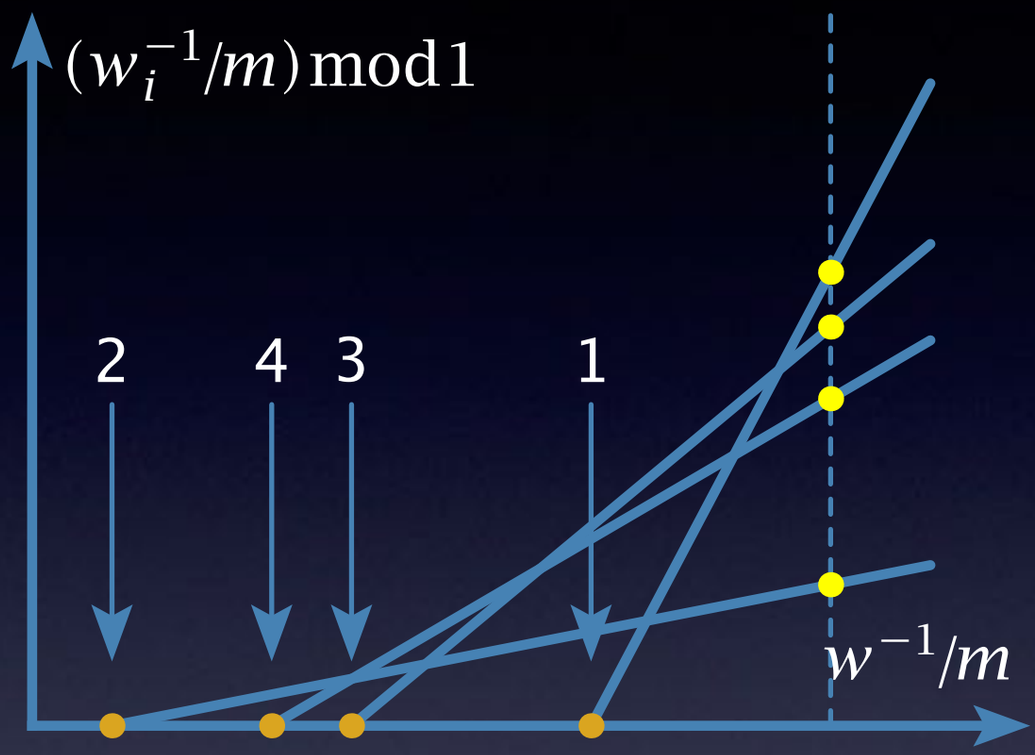
- verzender
  M *is* $x = (x_1,x_2,\ldots)$
  C is b.x $= b_1x_1+\ldots+b_nx_n$
- ontvanger
  $w^{-1}C = w^{-1}b.x \bmod m$
  $w^{-1}(b_1x_1+\ldots+b_nx_n) \bmod m$
  $w^{-1}(w.a_1x_1+\ldots+w.a_nx_n) \bmod m$
  $(a_1x_1+\ldots+a_nx_n) \bmod m = a.x$
  superstijgend splitst a

gebroken

- Adi Shamir, Crypto 1982

Shamir breekt Knapzak





- $a_1 \approx 2^{100} \ldots a_{100} \approx 2^{200} \rightarrow b_i \approx 2^{200}$
- reduceer met w_i^{-1}/m $b_1 \approx 2^{200} \rightarrow a_1 \approx 2^{100}$, idem b_2, etc.
- kans op cluster nulpunten $P_i \approx 2^{3n-ni+i(i-1)/2}$
- met i = 4, n = 100 $\rightarrow P_4 \approx 2^{-94}$
- zoek ze met Lenstra-Lenstra-Lovacz-algoritme