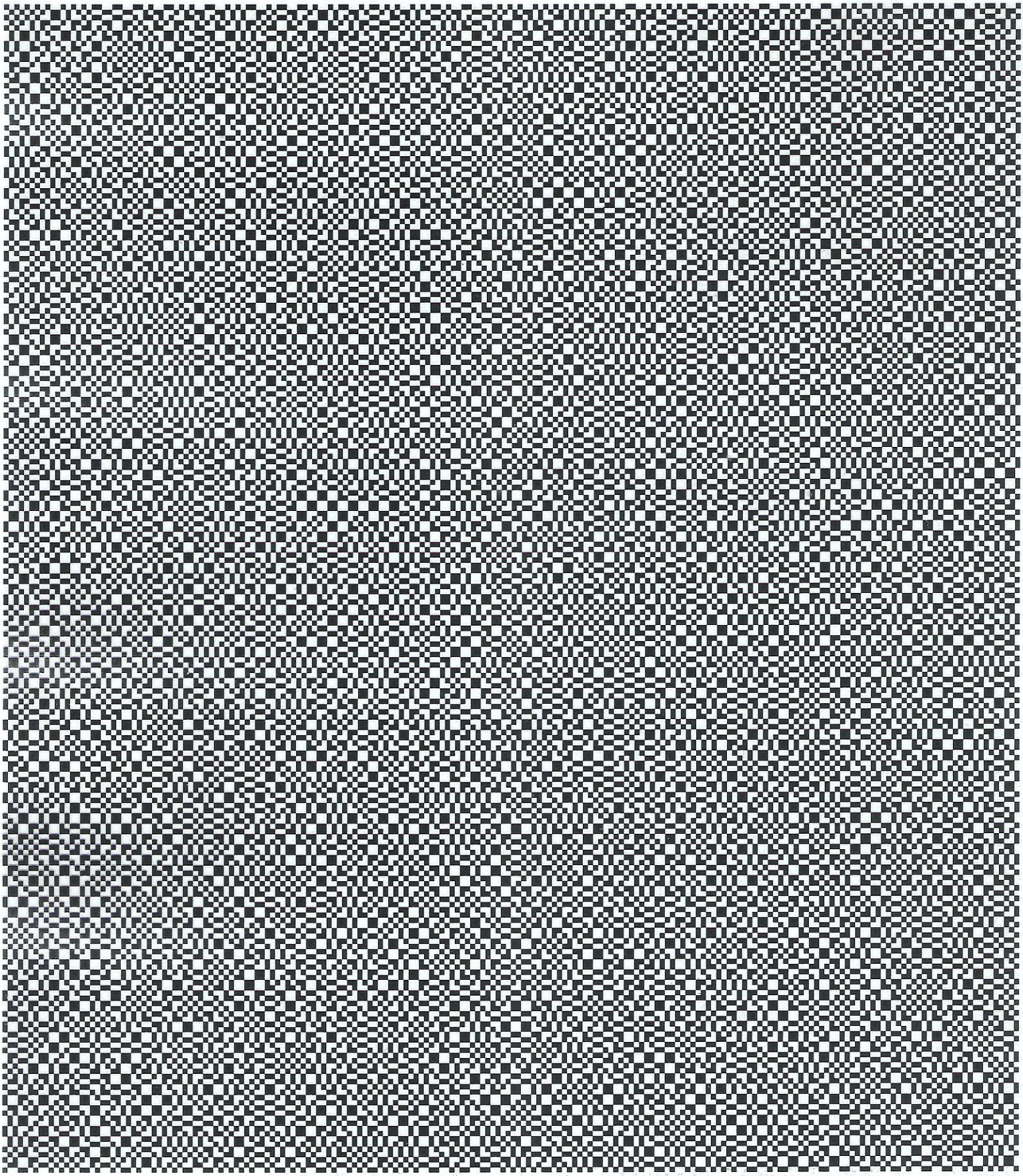
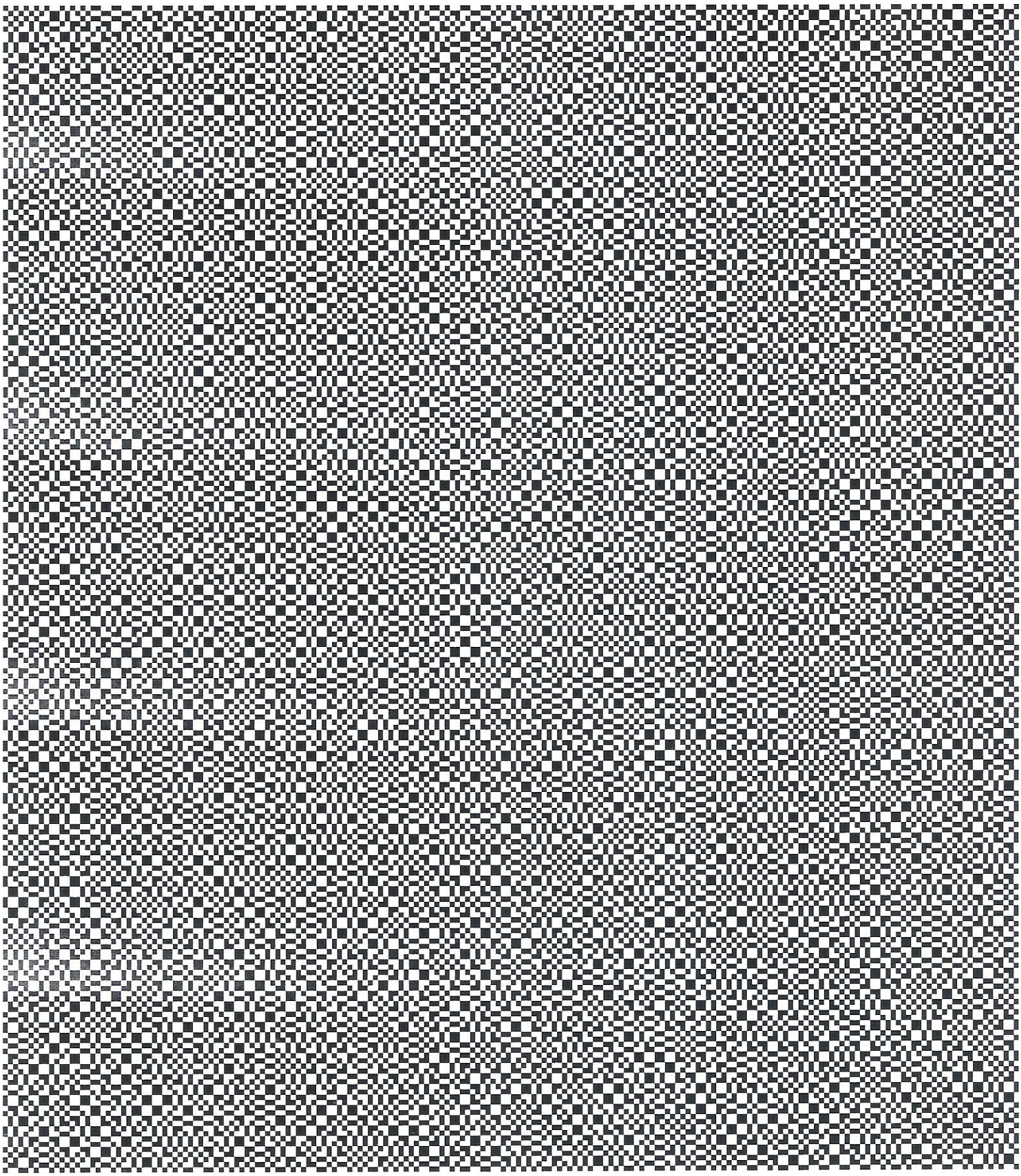
Die Methode Secret Splitting mit $k=n=2$ kann verstanden werden als Grundlage für Visuelle Kryptographie (ein klassisches Verfahren).

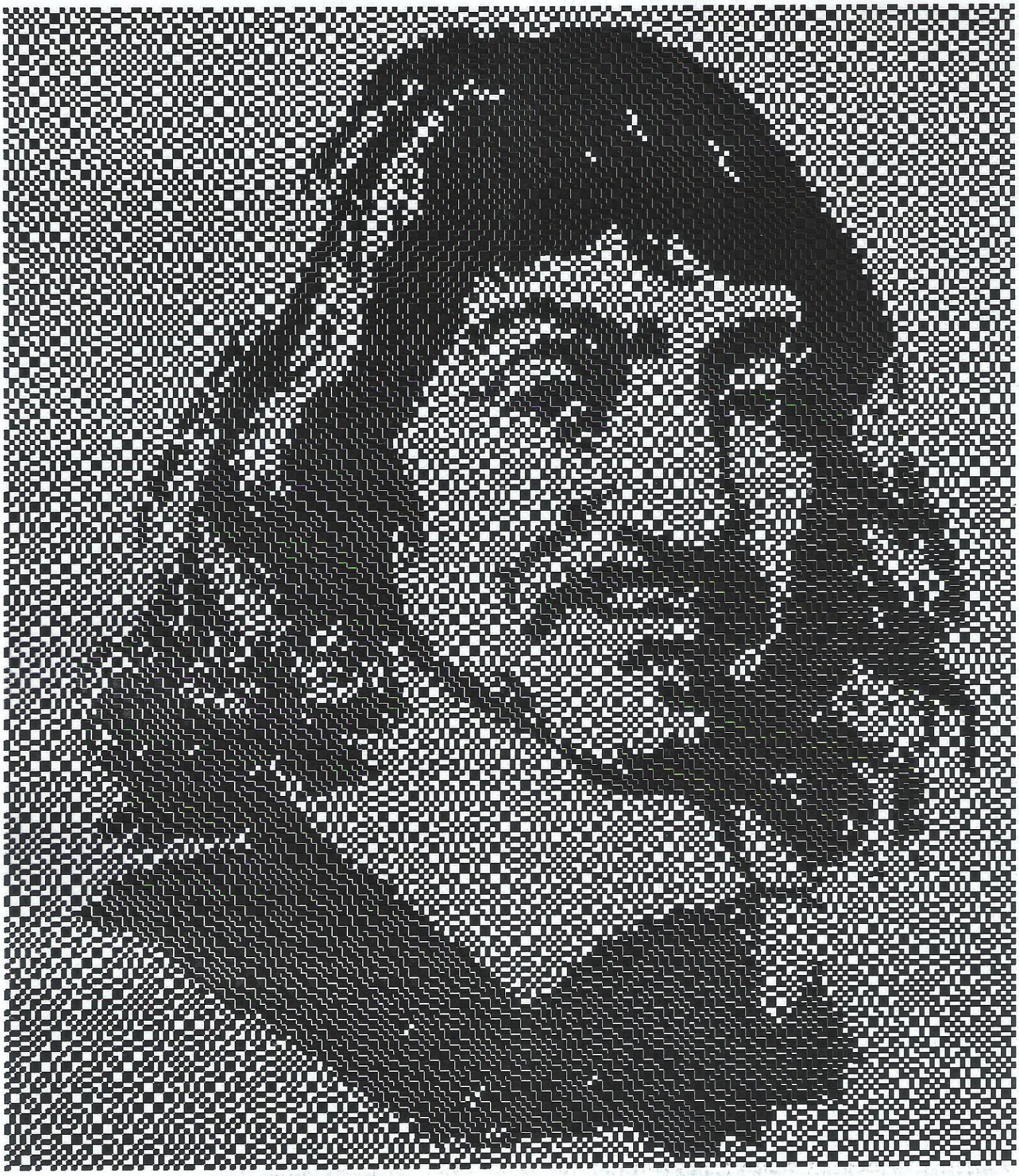
Die zu übertragende Nachricht ist ein Schwarz-Weiß-Bild:

Dieses wird in Weiße und Schwarze Pixel unterteilt.

Nun erzeugt man eine erste Folie mit rein zufälligen „Pixeln" der Art ▣ oder ▣. Die 2. Folie ist bei genau derjenigen „Pixeln" komplementär, wo das Originalbild schwarz ist, sonst sind die „Pixel" von 1. und 2. Folie identisch. Beim Übereinanderlegen der 2 Folien entsteht eine Oder-Verknüpfung. (Korrekt wäre eine XOR-Verknüpfung. Deshalb entsteht grau, wo das Original weiß ist.)







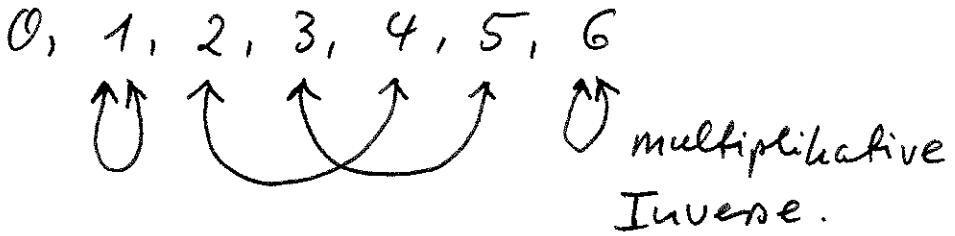
Beispiel: Ein (2,4)-Schwellenwertsystem. Man benötigt Polynome mit 2 Koeffizienten (lineare Funktionen):

$$p(x) = a + b \cdot x$$

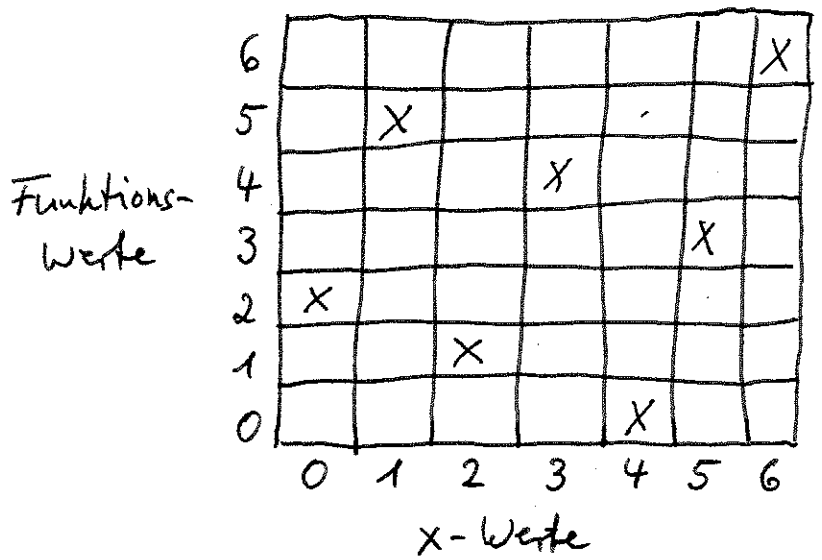
↑ das Geheimnis

Der probabilistische Algorithmus zur Erzeugen der 4 Teilgeheimnisse wählt z.B. das Polynom $p(x) = 2 + 3 \cdot x$.

Wir rechnen in GF(7); also modulo der Primzahl 7.



Die „Gerade" $2+3x$ sieht auf GF(7) so aus:



An die 4 Bankdirektoren werden die Teilgeheimnisse (1,5), (2,1), (3,4), (4,0) verteilt.

Wenn beispielsweise die beiden Teilgeheimnisse (1,5) und (3,4) beigesteuert werden, so kann man das Geheimnis ermitteln: In $y = a + bx$ die beiden Punkte einsetzen:

$$5 = a + b \cdot 1$$
$$4 = a + b \cdot 3$$

$a = 5 - b$ in 2. Gleichung einsetzen: (mod 7 rechnen!)

$$4 = (5-b) + 3b$$
$$\Leftrightarrow -1 = 2b$$
$$\Leftrightarrow b = -2^{-1}$$
$$\Leftrightarrow b = -4$$
$$\Leftrightarrow b = 3 \qquad \Rightarrow a = 5 - b = \underline{\underline{2}}$$

Wenn beispielsweise nur das Teilgeheimnis eines Teilnehmers vorliegt, etwa (2,1), so können (unter Gleichverteilung) die möglichen Geraden durch den Punkt (2/1) alle möglichen Achsenabschnitte $a = 0, 1, 2, 3, 4, 5, 6$ haben.

Verallgemeinerung aller Verfahren, die auf dem Diskreten Logarithmus (bzw. Exponentiation) beruhen (insbesondere Diffie-Hellman Schlüsselvereinbarung):

→ Man benötigt eine Grundmenge (bisher: $\mathbb{Z}_n^*$, n Primzahl) von Zahlen (allgemeiner: von mathematischen Strukturen), die beliebig skalierbar ist.

→ Auf diesen mathematischen Objekten muss eine Gruppenstruktur (mit einer Gruppenoperation $\circ$) existieren (bisher: Multiplikation mod n). Die Gruppenop. muss effizient berechenbar sein (und damit auch $a^n = a \circ a \circ \dots \circ a$; square+multiply).

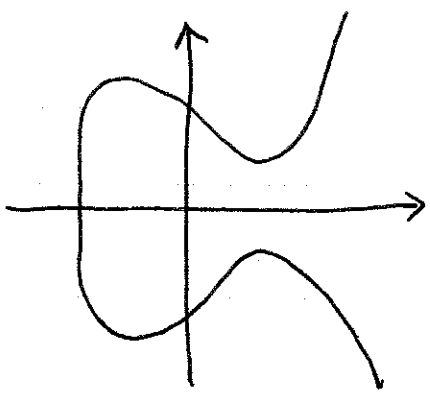
→ Bisher haben wir ein erzeugendes Element a (eine Primitivwurzel) verwendet. Es wäre ausreichend, wenn das Gruppenelement a eine sehr große Ordnung hätte, also so dass $\langle a \rangle$ eine sehr große Teilmenge der Gruppe ist. Zumindest: wenn ein zufällig gewähltes Element $a \in G$ mit hoher W'keit eine sehr große Ordnung hat.

Eine solche Situation lässt sich erreichen mittels elliptischer Kurven.

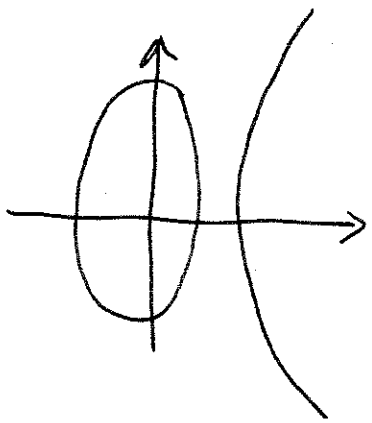
Eine elliptische Kurve über einem zugrunde liegenden Körper K sind folgende Punkte in K^2:

$$E_{a,b} = \{(x,y) \in K^2 \mid y^2 = x^3 + ax + b\}$$

Über dem Körper $\mathbb{R}$ haben elliptische Kurven folgendes Aussehen:



oder



falls $\left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 > 0$

$\Leftrightarrow 4a^3 + 27b^2 > 0$

falls $\left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 < 0$

$\Leftrightarrow 4a^3 + 27b^2 < 0$

Der Fall $4a^3 + 27b^2 = 0$ ist zu vermeiden.

Kleiner Einschub (aus Formelsammlung):

die Cardano'schen Formeln.

Gegeben kubische Gleichung: $x^3 + ax^2 + bx + c = 0$

(Normalform)

Man substituiert $x = z - \frac{a}{3}$ und erhält die

reduzierte Form: $z^3 + p \cdot z + q = 0$

wobei $p = \frac{3b - a^2}{3}$, $q = \frac{2a^3}{27} - \frac{ab}{3} + c$

Die sog. Diskriminante: $D = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$

Falls $D > 0$: eine reelle, 2 konj. komplexe Lösungen

" $D = 0$: drei reelle Lösungen, dabei 2 identische

" $D < 0$: drei verschiedene reelle Lösungen

Die Lösungen der reduzierten Form ergeben sich dann wie folgt:

$$z_1 = u + v$$

$$z_2 = -\frac{1}{2}(u+v) + \frac{1}{2}(u-v)\sqrt{3} \cdot i$$

$$z_3 = -\frac{1}{2}(u+v) - \frac{1}{2}(u-v)\sqrt{3} \cdot i$$

wobei $u = \sqrt[3]{-\frac{q}{2} + \sqrt{D}}$, $v = -\frac{p}{3u}$

Beispiel: Sei $K = \mathbb{Z}_{13} =$

$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$

der zugrunde liegende Körper.

Sei $a = 2$, $b = 3$, also $p(x) = 2 + 3 \cdot x$

Probe: $4 \cdot a^3 + 27 \cdot b^2 = 2 > 0$

$$E = \{ (x, y) \in \mathbb{Z}_{13}^2 \mid y^2 = x^3 + 2x + 3 \}$$

Die Quadratzahlen in $\mathbb{Z}_{13}$ sind:

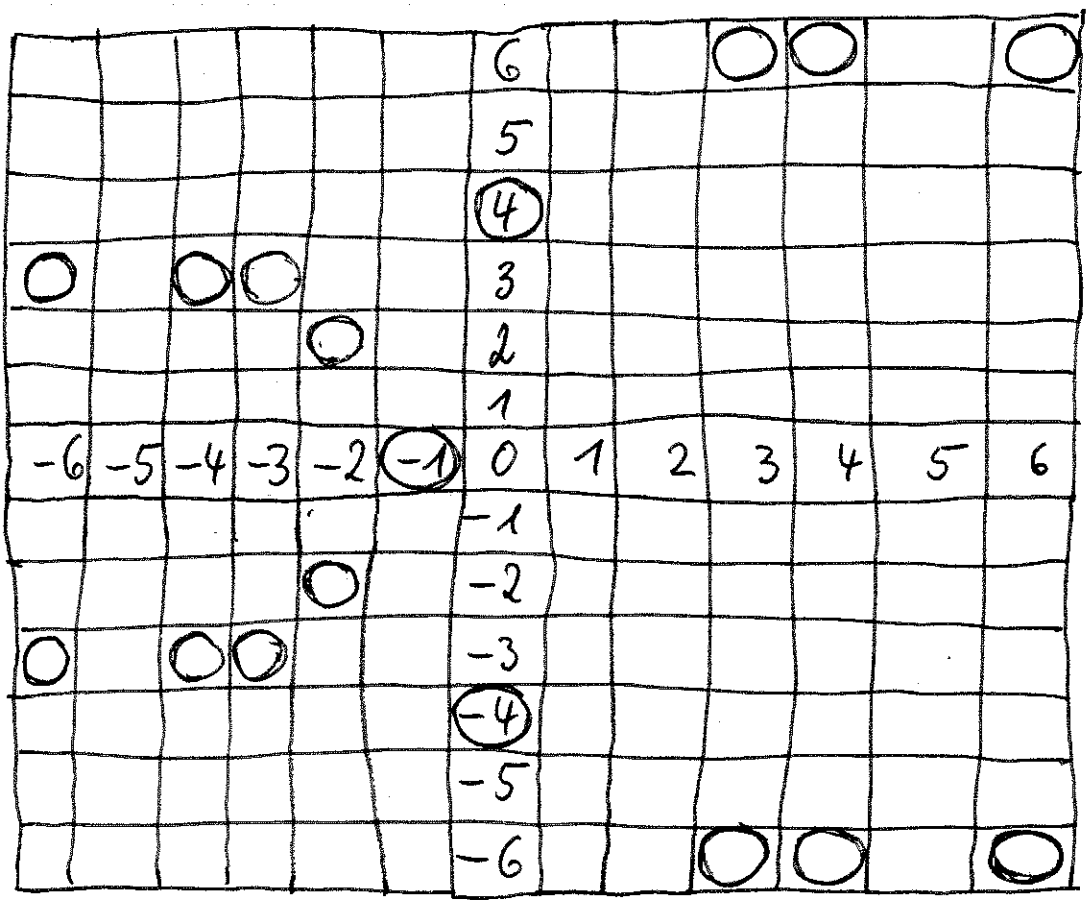
0	mit Q.Wurzel	0
1	——	1 und -1
3	——	4 und -4
4	mit Q. Wurzel	2 und -2
$-4 = 9$	——	3 und -3
$-3 = 10$	——	6 und -6
$-1 = 12$	——	5 und -5

$x =$	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
$x^2+2x+3 =$	9	11	9	9	4	0	3	6	2	10	10	8	10
Quadrat?	✓		✓	✓	✓	✓	✓			✓	✓		✓

Somit ist

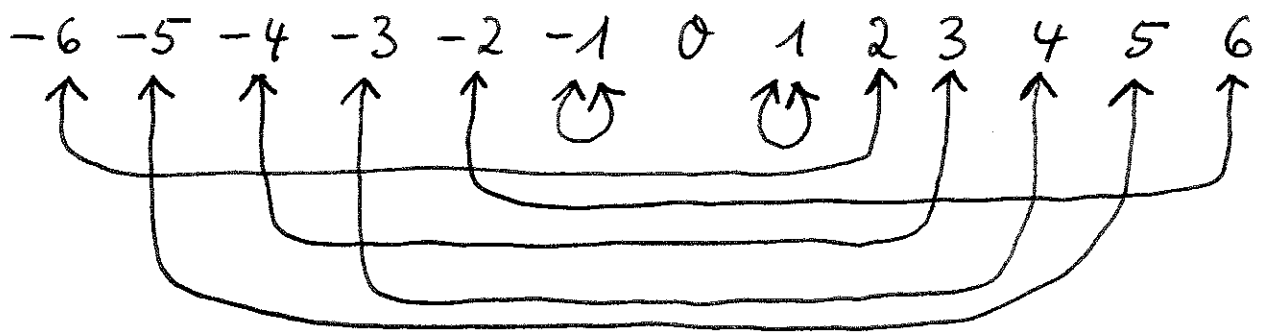
$$E = \{ (-6, \pm 3), (-4, \pm 3), (-3, \pm 3), (-2, \pm 2), (-1, 0), (0, \pm 4), (3, \pm 6), (4, \pm 6), (6, \pm 6) \}$$

Graphisch:



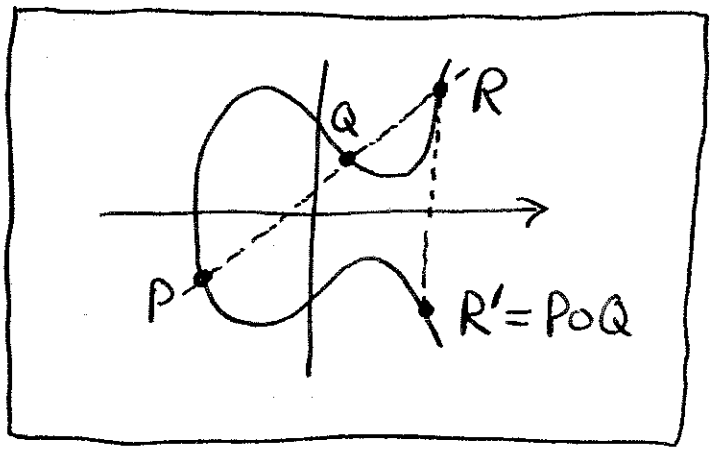
Grob: etwa jede 2. Zahl der Form $x^3 + ax + b$ ist Quadratzahl.
Für $E \subseteq \mathbb{Z}_n^2$ ist daher $|E| \approx n$.

Für späteren Gebrauch, die multiplikativen Inversen:



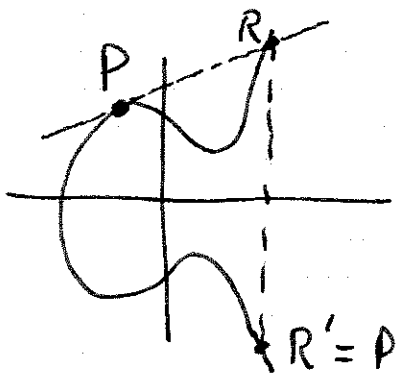
Auf der Menge der Punkte, die auf einer elliptischen Kurve liegen, soll nun eine Gruppen-Operation definiert werden. Seien P und Q zwei verschiedene Punkte. Dann gibt es immer genau einen dritten Punkt R, der die Kurve schneidet, wenn man eine Gerade durch PQ legt.

(Veranschaulichung auf $\mathbb{R}$)

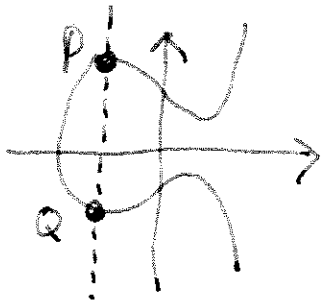


Symmetrisch zur x-Achse liegt dann ebenfalls ein Punkt auf der Kurve, den wir R' nennen. Genau diesen Punkt R' definieren wir als PoQ.

<u>Sonderfall</u> $P=Q$, d.h. es soll $P \circ P$ bestimmt werden. Dann legen wir eine <u>Tangente</u> an den Punkt P, bestimmen den weiteren Schnittpunkt R der Kurve mit der Tangenten, spiegeln R an der x-Achse, und der gespiegelte Punkt R' wird definiert als $P \circ P$.



Sonderfall: P und Q liegen senkrecht übereinander (d.h. $Q = P'$)



Dann gibt es keinen 3. Schnittpunkt der PQ-Gerade mit der Kurve. Wir fügen der Elliptischen Kurven-Punktemenge E einen weiteren, künstlichen Punkt $\mathcal{O}$ (sozusagen „im Unendlichen") hinzu, definieren in diesem Fall $P \circ Q = \mathcal{O}$.

Nun bildet $G = E \cup \{\mathcal{O}\}$ tatsächlich eine Gruppe mit $\mathcal{O}$ als dem neutralen Element:

$$P \circ \mathcal{O} = P \; , \quad \mathcal{O} \circ P = P$$

sowie $P \circ Q = \mathcal{O}$, falls P, Q senkrecht aufeinander liegen. Das bedeutet in dieser Gruppenstruktur nämlich, dass P und Q inverse zueinander sind. Tatsächlich kann man aus den Punktkoordinaten $P = (x_1 | y_1)$ und $Q = (x_2 | y_2)$

die Koordinaten von $P \circ Q = (x_3 / y_3)$

analytisch berechnen (sofern das Ergebnis nicht $\mathcal{O}$ ist):

Setze $$\lambda = \begin{cases} (y_2 - y_1) \cdot (x_2 - x_1)^{-1}, & \text{falls } P_1 \neq P_2 \\ (3 \cdot x_1^2 + a) \cdot (2 \cdot y_1)^{-1}, & \text{falls } P_1 = P_2 \end{cases}$$

(Diese Rechnungen finden im Körper K statt, sowie $E_{a,b} \subseteq K^2$).

Dann ist $$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda \cdot (x_1 - x_3) - y_1$$

<u>Rechenbeispiel:</u> Betrachte $E = E_{2,3}$ von oben, also $a=2$, $b=3$. Seien $P = (-4/-3)$, $Q = (-2/2) \in E$.

Dann ist $(y_2 - y_1) = 2+3 = 5$, $(x_2 - x_1) = -2+4 = 2$,

$(x_2 - x_1)^{-1} = 2^{-1} = -6$, $(y_2 - y_1) \cdot (x_2 - x_1)^{-1} = 5 \cdot (-6)$

$= -30 = -4 = \lambda$, $x_3 = \lambda^2 - x_1 - x_2 = (-4)^2 + 4 + 2 = -4$

$y_3 = \lambda \cdot (x_1 - x_3) - y_1 = -4 \cdot (-4+4) + 3 = 3$.

Somit ist $P \circ Q = (-4/3) \in E$.

Berechnen wir noch $P^2 = P \circ P$, wobei

$P = (-4/-3)$.

$(3 \cdot x_1^2 + a) = 3 \cdot (-4)^2 + 2 = 11 = -2$

$(2 \cdot y_1)^{-1} = (-6)^{-1} = 2$

$(3 \cdot x_1^2 + a) \cdot (2y_1)^{-1} = (-2) \cdot 2 = -4 = \lambda$

$x_3 = \lambda^2 - x_1 - \overset{x_1}{x_2} = (-4)^2 + 4 + 4 = 11 = -2$

$y_3 = \lambda \cdot (x_1 - x_3) - y_1 = -4 \cdot (-4+2) - x_3 = 11 = -2$

$\Rightarrow P \circ P = (-2/-2)$

Da man die $\circ$-Operation mit einigen Additionen, Subtraktionen, Multiplikationen und Inversen-Berechnungen über $\mathbb{Z}_n^*$ ausrechnen kann (Laufzeit: $O(m^2)$), kann man auch die Operation $P^n = \underbrace{P \circ P \circ \dots \circ P}_{n\text{-mal}}$ effizient berechnen; wie gehabt: mit der Methode „Square-and-multiply".

Da die inversen Elemente gerade $P = (x/y)$ und $P' = (x/-y)$ sind, ist man geneigt

für $(x|-y)$ zu schreiben: $-P$.

Dementsprechend wird in der Literatur die $\circ$-Operation eher als „Addition" von Punkten verstanden (anstatt als „Multiplikation"; an den Formeln ändert sich gar nichts, nur an der Nomenklatur).

Dann versteht man $P \circ P \circ \ldots \circ P$ als n-fache „Addition" und schreibt dafür dementsprechend nP. Statt Methode „square-and-multiply" sagt man nun „double-and-add".

Bem: Wenn man Kryptosysteme, die auf Faktorisieren beruhen, mit 1000 Bit-Schlüsseln, bei Diskretem Log mit 500-Bit-Schlüsseln als ähnlich sicher (Sicherheitsniveau ≥ 80 Bit) betrachten kann, dann erreicht man ähnliche Sicherheit bei elliptischen Kurven bereits bei ca. $n = 160$.