Secret Sharing

Olav Geil
Institut for Matematiske Fag
Aalborg Universitet
email: olav@math.aau.dk
URL: http://www.math.aau.dk/~olav

September 2006

1 Læsevejledning

Nærværende note er tænkt som et oplæg til 3. g opgave i matematik. Noten er udformet således, at man kan gå mere eller mindre i dybden med emnet. Som minimum skal man arbejde med afsnittene 2, 3, 6 og 7. Vælges denne barberede version kan man ikke regne alle opgaverne i afsnit 7. Øvrige afsnit kan tilvælges efter ønske. Resultaterne i afsnit 5 kan eventuelt tages for gode varer uden bevis.

2 Problemstillingen

I en bank er der fem bankdirektører. Man ønsker den elektroniske lås på et pengeskab indrettet således, at hvis vilkårlige tre bankdirektører indtaster deres koder samtidig, da kan de åbne skabet. Er der blot en eller to tilstede, da skal skabet være umuligt at åbne. Et nøglesystem, som kan klare en sådan opgave vil vi kalde et "secret sharing scheme". Mere generelt vil vi betragte situationen, hvor der er n direktører og hvor k skal være tilstede, for at låsen kan åbnes. Her kan k antage alle værdier fra 1 op til n. Det er muligt at betragte endnu mere sofistikerede situationer, hvor nogle direktører har flere nøgler, mens andre blot har en enkelt. Dette vil dog ikke blive behandlet i denne note.

3 Alle skal være tilstede

I situationen, hvor alle bankdirektører skal være tilstede på samme tid, kunne vi forestille os følgende secret sharing scheme. Bankdirektørerne b_1, b_2, b_3, b_4, b_5 får tildelt koderne s_1, s_2, s_3, s_4, s_5, som alle er hele tal mellem 0000 og 1999. Den hemmelige nøgle, som kan åbne låsen er nu $s = s_1 + s_2 + s_3 + s_4 + s_5$. Dette secret sharing scheme løser delvist opgaven, men ikke helt. Antag nemlig, at kun personerne b_1, b_2, b_3, b_4 er tilstede. De kan selvfølgelig ikke vide, hvad s_5 er, og dermed ved de heller ikke hvad s er. Men de ved, at s er mindst lig $s_1 + s_2 + s_3 + s_4$ og højst lig $s_1 + s_2 + s_3 + s_4 + 1999$ og med denne viden kan de begynde at gætte på, hvad s er. Dette er en uheldig egenskab og vi vil derfor forlange af vores secret sharing scheme, at hvis færre end fem direktører er tilstede, da skal de absolut ingen information have om den hemmelige nøgle s. Som vi skal se i det følgende giver matematikken os en smart løsning på problemet.

Det værktøj vi vil benytte, kaldes modulær regning. Vi starter med et eksempel.

Bankdirektørerne b_1, b_2, b_3, b_4, b_5 tildeles nu i stedet koderne s_1, s_2, s_3, s_4, s_5, som alle er hele tal mellem 0000 og 9999. Den hemmelige nøgle s findes nu som de sidste fire cifre i tallet $s_1 + s_2 + s_3 + s_4 + s_5$. Altså, hvis $s_1 = 2856$, $s_2 = 7700$, $s_3 = 0056$, $s_4 = 9918$ og $s_5 = 9879$ da fås $s_1 + s_2 + s_3 + s_4 + s_5 = 30409$ og dermed er den hemmelige nøgle lig $s = 0409$. Dette system har den ønskede egenskab, at ingen gruppe bestående af færre end fem direktører har nogen form for viden om, hvad den hemmelige kode er.

Vi indfører nu modulær regning generelt. Lad a og m være positive heltal. Skriv $a = qm + r$, hvor q er et ikke negativt heltal og r er heltal i intervallet $[0, \ldots m-1]$. Altså hvis $a = 9$ og $m = 4$ så fås $q = 2$ og $r = 1$ fordi $9 = 2 \cdot 4 + 1$. Tilsvarende hvis $a = 30409$ og $m = 10000$ så fås $q = 3$ og $r = 409$. Vi vil skrive $r = a$ rem m. Så 9 rem $4 = 1$ og 30409 rem $10000 = 409$. Med ord siger vi, at 9 rest modulo 4 er 1 og, at 30409 rest modulo 10000 er 409.

Med den modulære regning i hånden kan vi forklare lidt mere formelt, hvorfor de fire bankdirektører i ovenstående eksempel ingen viden har om den hemmelige nøgle s. Summen af koderne s_1, s_2, s_3, s_4 er 20530. Men

$$\begin{aligned}
20530 + 0 \quad &\text{rem} \quad 10000 \quad = 530 \\
20530 + 1 \quad &\text{rem} \quad 10000 \quad = 531 \\
&\vdots \\
20530 + 9469 \quad &\text{rem} \quad 10000 \quad = 9999 \\
20530 + 9470 \quad &\text{rem} \quad 10000 \quad = 0 \\
20530 + 9470 \quad &\text{rem} \quad 10000 \quad = 1 \\
&\vdots \\
20530 + 9998 \quad &\text{rem} \quad 10000 \quad = 528 \\
20530 + 9999 \quad &\text{rem} \quad 10000 \quad = 529
\end{aligned}$$

udgør tallene $0, \ldots, 9999$. Så uden viden om s_5 kan s ligeså godt være det ene som det andet.

I forbindelse med modulære udregninger kan man have glæde af følgende regneregel: $(a+b)$ rem $m = ((a \text{ rem } m)+(b \text{ rem } m))$ rem m. Altså for eksempel $20530 + 1$ rem $10000 = 530 + 1$ rem $10000 = 531$.

Vi afslutter dette afsnit med et eksempel, hvor vi i stedet for at regne modulo 10000 regner modulo 13. Lad der være 3 bankdirektører b_1, b_2 og b_3. De får nøglerne $s_1 = 5$, $s_2 = 4$ og $s_3 = 5$. Den hemmelig nøgle er nu $5+4+5$ rem $13 = 1$. Kun hvis alle tre direktører er tilstede kan nøglen genereres.

4 Legemet $\mathbb{Z}_5$

I det mest generelle set-up i denne note får vi brug for at regne i såkaldte legemer $\mathbb{Z}_p$, hvor p er et primtal. I dette afsnit ser vi nærmere på situationen, hvor der

regnes modulo 5. Konstruktionen generaliseres umiddelbart til tilfældet, hvor p er et primtal forskelligt fra 5. Betragt $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Vi har $3 + 4 = 7$, men 7 er jo ikke et element i $\mathbb{Z}_5$, så hvordan skal vi definere + på $\mathbb{Z}_5$? Svaret er enkelt. Vi siger $3 + 4 = 2$ fordi 7 rem $5 = 2$. Vi får følgende additionstabel.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Vi har $0+0=0$, $1+4=0$, $2+3=0$, $3+2=0$ og $4+1=0$. Vi skriver derfor $-0=0$, $-1=4$, $-2=3$, $-3=2$ og $-4=1$.

På samme måde er $3 \cdot 2 = 6$ jo heller ikke et element i $\mathbb{Z}_5$, så vi definerer $3 \cdot 2 = 1$ fordi 6 rem $5 = 1$. Vi får følgende multiplikationstabel.

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Vi har $1 \cdot 1 = 1$, $2 \cdot 3 = 1$, $3 \cdot 2 = 1$ og $4 \cdot 4 = 1$. Vi skriver $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$ og $4^{-1} = 4$.

5 Legemer

Strukturen $\mathbb{Z}_5$ fra afsnit 4 har mange ligheder med de velkendte strukturer $\mathbb{Q}$ og $\mathbb{R}$. Her er $\mathbb{Q}$ de rationale tal (brøkerne) og $\mathbb{R}$ er de reelle tal. Såvel $\mathbb{Z}_5$, $\mathbb{Q}$ og $\mathbb{R}$ er eksempler på såkaldte legemer.

Definition 1
En mængde L med tilhørende regneoperationer + og $\cdot$ (kaldet plus og gange) er et legeme, hvis følgende er opfyldt:

(1) for alle x, y gælder $x + y = y + x$
(2) for alle x, y, z gælder $(x + y) + z = x + (y + z)$
(3) for alle x gælder $x + 0 = x$
(4) for alle x findes der element $-x$ så $x + (-x) = 0$
(5) for alle x, y gælder $x \cdot y = y \cdot x$
(6) for alle x, y, z gælder $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
(7) for alle x gælder $x \cdot 1 = x$
(8) for alle $x \neq 0$ findes der element x^{-1} så $x \cdot x^{-1} = 1$
(9) for alle x, y, z gælder $x \cdot (y + z) = x \cdot y + x \cdot z$

Opgave 1
Eftervis, at $\mathbb{Z}_5$ er et legeme.

Definition 2
Givet et primtal p lad $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Definer $+$ og $\cdot$ som i afsnit 4. Altså, lad $a + b = (a + b)$ rem p og lad $a \cdot b = ab$ rem p.

Sætning 1
$\mathbb{Z}_p$ er et legeme.
Bevis: Man skal eftervise at (1), (2), ... , (9) i Definition 1 holder. Vi efterviser blot (4) og (8), som er de sværeste.
Først eftervises (4). Hvis $a = 0$, så opfylder $-a = 0$ betingelsen, fordi $0 + 0$ rem $p = 0$. Lad nu $a \in \{1, 2, \ldots, p-1\}$. Men så opfylder elementet $p - a$, at $a + (p - a) = p$ rem $p = 0$ og derfor er $-a = p - a$.
Dernæst eftervises (8). Lad $a \in \{1, 2, \ldots, p-1\}$. Vi skal vise, at der findes et tal $b \in \{1, 2, \ldots, p-1\}$, så $a \cdot b = 1$. Betragt tallene $a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$. Da p ikke går op i nogle af ovenstående tal, da er disse alle forskellige fra 0 (i $\mathbb{Z}_p$). Vi viser nu, at tallene er parvist forskellige, og derfor må et af dem være lig 1. Antag, at to er ens, altså at as rem $p = at$ rem p for $s \neq t$, $s, t \in \{1, 2, \ldots, p-1\}$. Men så $p \mid (as - at)$ og dermed $p \mid (a(s - t))$. Det følger, at $p \mid (s - t)$. Men dette er umuligt, da $s - t$ er et heltal i $\{-(p-2), -(p-3), \ldots, -1, 1, 2, \ldots p-2\}$.

Opgave 2
Færdiggør beviset for Sætning 1.

Fra beviset for forrige sætning får vi følgende vigtige resultat.

Sætning 2
Lad $a \in \mathbb{Z}_p \backslash \{0\}$, så er $a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$ parvist forskellige. Alle er forskellige fra 0.

6 Lagrange-interpolation

I næste afsnit vil vi præsentere Shamirs secret sharing scheme i tilfældet, hvor der er givet tre bankdirektører, men hvor to alene har lov at åbne pengeskabet. Vi får brug for Lagrange-interpolation, der er en metode til at finde et polynomium $f(x)$ af grad højst 1 som tilfredstiller, at $f(a) = c$ og at $f(b) = d$.[1]

Sætning 3
Polynomiet

$$f(x) = \frac{x-b}{a-b}c + \frac{x-a}{b-a}d \tag{1}$$

[1] I sin mere generelle form finder Lagrange-interpolation et polynomium af grad højst $k-1$, som tilfredstiller $f(u_1) = v_1, \ldots, f(u_k) = v_k$. Dette kan benyttes til at opstille et secret sharing scheme, hvor vilkårlige k bankdirektører ud af en gruppe på n bankdirektører kan genskabe den hemmelige nøgle.

opfylder $f(a) = c$ samt $f(b) = d$. Det er det eneste polynomium af grad højst 1, som gør dette.

Bevis: Første del vises ved indsættelse. For at bevise anden del antager vi, at der er to forskellige løsninger f og g. Men så fås $(f-g)(a) = 0$ og $(f-g)(b) = 0$, hvilket er umuligt, da et ikke-nul polynomium af grad højst 1 højst kan have et nulpunkt.

□

Vi starter med et eksempel, hvor der regnes med reelle tal. Vi søger polynomiet $f(x)$ af grad højst 1, så $f(3) = 2$ og $f(4) = 6$. Ifølge sætningen ovenfor er der præcis en løsning til dette problem, og denne løsning er af formen

$$\begin{aligned} f(x) &= \frac{x-4}{3-4}2 + \frac{x-3}{4-3}6 \\ &= -2x + 8 + 6x - 18 \\ &= -10 + 4x \end{aligned}$$

Herefter fortsætter vi med et eksempel over $\mathbb{Z}_5$. For at kunne forstå dette eksempel, er det en forudsætning at afsnittet 4 er arbejdet igennem. Man kan eventuelt springe følgende eksempel over.

Vi søger polynomiet $A + Bx$, hvor $A \in \mathbb{Z}_5$ og $B \in \mathbb{Z}_5$ og hvor $f(3) = 2$ og $f(4) = 1$ (udregninger foretaget i $\mathbb{Z}_5$). Ifølge sætningen ovenfor er der præcis en løsning til dette problem, og denne løsning er af formen

$$\begin{aligned} f(x) &= \frac{x-4}{3-4}2 + \frac{x-3}{4-3}1 \\ &= \frac{x+1}{3+1}2 + \frac{x+2}{4+2}1 \\ &= \frac{x+1}{4}2 + \frac{x+2}{1} \\ &= (x+1)4^{-1} \cdot 2 + (x+2) \cdot 1^{-1} \\ &= (x+1)4 \cdot 2 + (x+2)1 \\ &= (x+1)3 + (x+2) \\ &= 3x + 3 + x + 2 \\ &= 4x + 5 \\ &= 4x \end{aligned}$$

7 Shamirs secret sharing scheme

I dette afsnit behandles Shamirs secret sharing scheme i det tilfælde, hvor der er tre bankdirektører, men to alene har lov at åbne pengeskabet. Metoden gør

brug af Lagrange-interpolationen fra forrige afsnit. I praksis vil man arbejde med legemer $\mathbb{Z}_p$, hvor p er et stort primtal. Her gennemgår vi metoden, som den tager sig ud over de reelle tal. Læsereren kan selv prøve at generalisere til tilfældet, hvor der regnes over $\mathbb{Z}_5$ eller mere generelt, hvor der regnes over $\mathbb{Z}_p$. Metoden kan generaliseres til at håndtere situationen med n bankdirektører, hvor k skal være tilstede, for at pengeskabet kan åbnes.

Lad den hemmelige nøgle være lig med $f_0 = -10$. Vi vælger f_1 tilfældigt til at være $f_1 = 4$. Herudfra konstrueres polynomiet $f_0 + f_1 x = -10 + 4x$ (som holdes hemmeligt overfor bankdirektørerne). Direktør b_1 får at vide, at $f(3) = 2$. Direktør b_2 får at vide, at $f(4) = 6$. Direktør b_3 får at vide, at $f(2) = -2$. Ud fra dette kan b_1 og b_2 ifølge forrige afsnit rekonstruere $f_0 + f_1 x = -10 + 4x$ og dermed har de fundet ud af, at den hemmelige nøgle er lig -10. Tilsvarende kunne b_1 og b_3 henholdsvis b_2 og b_3 benytte metoden fra forrige afsnit og bestemme f_0 til at være -10.

Opgave 3 Udfør Lagrange interpolationen for b_1 og b_3. Udfør derefter Lagrange interpolationen for b_2 og b_3. Du skal meget gerne nå frem til $f_0 = -10$ hver gang.

Opgave 4 Regn over $\mathbb{Z}_5$. Hemmelig nøgle er $f_0 = 0$. Vi vælger tilfældigt $f_1 = 4$ og fortæller b_1, at $f(3) = 2$, fortæller b_2, at $f(4) = 1$ og fortæller b_3, at $f(2) = 3$. Udfør Lagrange interpolationen for b_1 og b_3. Udfør dernæst Lagrange interpolationen for b_2 og b_3

Opgave 5 Betragt interpolation over $\mathbb{Z}_5$. Udregn konstantleddet i (1) og argumenter herudfra for, at en bankdirektør alene ingen information har om, hvad f_0 er.

Opgave 6 Argumenter for, at det er essentielt, at direktørerne b_1, b_2 og b_3 interpolerer i forskellige punkter. Argumenter for, at det er essentielt, at ingen af disse punkter er 0.

Opgave 7 Genereliser metoden fra dette afsnit til at gælde i $\mathbb{Z}_p$, hvor p er et primtal. Besvar opgave 5 i dette mere generelle set-up (du får brug for resultaterne fra afsnit 5).

8 Shamirs secret sharing scheme i den generelle version

Den generelle version af Lagrangeinterpolation er som følger. Lad $f(x)$ være et polynomium af grad højst $k-1$, som opfylder

$$\begin{aligned} f(u_1) &= v_1 \\ f(u_2) &= v_2 \\ &\vdots \\ f(u_k) &= v_k \end{aligned} \tag{2}$$

Her er det antaget, at $u_1, u_2, \ldots, u_k$ er parvist forskellige. Man kan finde $f(x)$ ud fra følgende formel

$$\begin{aligned} f(x) &= \frac{(x-u_2)(x-u_3)\cdots(x-u_k)}{(u_1-u_2)(u_1-u_3)\cdots(u_1-u_k)}v_1 \\ &\quad + \frac{(x-u_1)(x-u_3)\cdots(x-u_k)}{(u_2-u_1)(u_2-u_3)\cdots(u_2-u_k)}v_2 \\ &\quad + \cdots \\ &\quad + \frac{(x-u_1)(x-u_2)\cdots(x-u_{k-1})}{(u_k-u_1)(u_k-u_2)\cdots(u_k-u_{k-1})}v_{k-1} \end{aligned}$$

Opgave 8
Eftervis at ovenstående polynomium opfylder $f(u_1) = v_1$, $f(u_2) = v_2, \ldots, f(u_k) = v_k$.

Opgave 9
Lad p være et primtal og lad k være et heltal, $1 < k < p$. Genereliser secret sharing schemet fra afsnit 7 på en sådan måde, at vilkårlige k bankdirektører kan generere hemmeligheden, men ingen mængde af $k-1$ har nogen viden om hemmeligheden.

Opgave 10
Gentag opgave 7 i dette generelle set-up.