Fiat-shamir, 4-Stellig

Fiat–Shamir–Verfahren Haftendorn 2012, www.mathematik–verstehen.de

Vorbereitungsphase: zwei Primzahlen (**unt**:=1 ▸ 1 ,RandSeed 2503)

p:=**kry\nextprime**(randInt(10^**unt**,10^**unt**+1)) ▸ 83

q:=**kry\nextprime**(randInt(10^**unt**,10^**unt**+1)) ▸ 59

n:=**p**·**q** ▸ 4897

s:=randInt(10^**unt**,**n**−2) ▸ 828 gcd(**s**,**n**) ▸ 1 (1, anderenfalls neu!)

v:=mod(**s**^2,**n**) ▸ 4

Anton gibt **v** ▸ 4 und **n** ▸ 4897 bekannt.

Anwendungsphase: 1. Antons Tat: er wählt r teilerfremd zu n und berechet x

r:=randInt(10^**unt**,**n**−2) ▸ 1085 gcd(**r**,**n**) ▸ 1 (1, anderenfalls neu!)

x:=mod(**r**^2,**n**) ▸ 1945 Anton sendet x an Berta.

1.1

Anton hat $v \blacktriangleright 4$ **und** $n \blacktriangleright 4897$ **und** $x \blacktriangleright 1945$ gesendet

2. Bertas Tat Berta empfängt x und sendet b=0 oder b=1 $b:=randint(0,1) \blacktriangleright 1$

3. Antons Reaktion empfängt x und antwortet mit y

$y:=ifFn(b=0,r,mod(r\cdot s,n)) \blacktriangleright 2229$

4. Bertas Test Berta quadriert y und erhält ihre Testzahl $test:=mod(y^2,n) \blacktriangleright 2883$
Diese vergleicht sie mit x oder x*v, je nachdem sie b=0 oder b=1 gesendet hatte.

$erg:=ifFn(b=0,ifFn(test=x,"ok","Käse"),ifFn(test=mod(x\cdot v,n),"gut","Quark")) \blacktriangleright$ gut

In Kurzform $test=x\cdot v^{b}$. Nun wird das Verfahren m-mal hintereinander ausgeführt. Siehe Tabellenfesnter. Die Wahrscheinlichleit, dass Anton rein zufällig Erfolg hat, ist

$\frac{1}{2^m} \blacktriangleright 2^{-m}$. wird geprüft. **Beweis der Durchführbarkeit:**

$test=y^2=(r\cdot s^b)^2=r^2\cdot s^{2b}=x\cdot (s^2)^b=x\cdot v^b$ q.e.d.

1.2

	A bit	B lir	C lix	D liy	E litest	F litestre	G	H
◆	=seq(rand	=seq(rand	=mod(lir^2	=mod(lir*'s	=mod(liy^2,'	=mod(lix*'		
1	1	2235	285	2235	285	285		
2	1	3942	1183	3942	1183	1183		
3	0	2701	3768	2701	3768	3768		
4	1	2432	3945	1029	1089	1089		
5	0	3677	4609	3677	4609	4609		
6	1	3443	3509	750	4242	4242		
7	0	1287	1183	2987	4732	4732		
8	0	903	2507	3340	234	234		
9	1	4585	4301	1205	2513	2513		
10	0	2036	2434	1240	4839	4839		
11	1	4205	3855	4870	729	729		
12	1	830	3320	1660	3486	3486		
13	0	4706	2202	4706	2202	2202		
14	0	461	1950	4639	2903	2903		
15	0	1739	2672	174	894	894		

A1 =1

1.3

Fiat-Shamir 12-stellig

Fiat–Shamir–Verfahren Haftendorn 2012

Vorbereitungsphase: zwei Primzahlen (**unt**:=4 ▸ 4 ,RandSeed 2503)

p:=**kry\nextprime**(randInt(10^**unt**,10^**unt**+2)) ▸ 19991

q:=**kry\nextprime**(randInt(10^**unt**,10^**unt**+2)) ▸ 440849

n:=**p**·**q** ▸ 8813012359

s:=randInt(10^**unt**,**n**−2) ▸ 7558985740 gcd(**s**,**n**) ▸ 1 (1, anderenfalls neu!)

v:=mod(**s**^2,**n**) ▸ 1907270014

Anton gibt **v** ▸ 1907270014 und **n** ▸ 8813012359 bekannt.

Anwendungsphase: 1. Antons Tat: er wählt r teilerfremd zu n und berechet x

r:=randInt(10^**unt**,**n**−2) ▸ 7045081279 gcd(**r**,**n**) ▸ 1 (1, anderenfalls neu!)

x:=mod(**r**^2,**n**) ▸ 4179856319 Anton sendet x an Berta.

2.1

Anton hat $v \blacktriangleright 1907270014$ **und** $n \blacktriangleright 8813012359$ **und** $x \blacktriangleright 4179856319$ gesendet

2. Bertas Tat Berta empfängt x und sendet b=0 oder b=1 $b:=\text{randint}(0,1) \blacktriangleright 0$

3. Antons Reaktion empfängt b und antwortet mit y

$y:=\text{mod}(r\cdot s^{b},n) \blacktriangleright 7045081279$

4. Bertas Test Berta quadriert y und erhält ihre Testzahl

$test:=\text{mod}(y^{2},n) \blacktriangleright 4179856319$ Diese vergleicht sie mit $x\cdot v^{b}$.

$erg:=\text{ifFn}(b=0,\text{ifFn}(test=x,\text{"ok"},\text{"Käse"}),\text{ifFn}(test=\text{mod}(x\cdot v,n),\text{"gut"},\text{"Quark"})) \blacktriangleright$ ok

Als Kurzform $test=x\cdot v^{b} \blacktriangleright$ true

Beweis der Durchführbarkeit

$test=y^{2}=(r\cdot s^{b})^{2}=r^{2}\cdot s^{2b}=x\cdot (s^{2})^{b}=x\cdot v^{b}$ q.e.d.

2.2

Angriffe, direkt

Angriffe auf das Fiat–Shamir–Verfahren

Anton hat $n:=2183 \blacktriangleright 2183$ und $v:=1705 \blacktriangleright 1705$ bekanntgegeben.

Um dies mit Punkten darzustellen, muss n unter 2500 liegen. Unter kann man dies ändern. Beim Neustart, sind es wieder andere Zahlen.

1. Betrugsversuch von Mister X, Geheimnis ausspähen

$v=\mathrm{mod}(s^2,n)$ also versucht Mister X die Quadratwurzel aus v zu ziehen.

Die modulare Wurzel kann man aber nicht so einfach nicht ziehen.

Im Tabellenfenster ist eine Liste mit allen Quadraten erzeugt.

Das Ergebnis v kann man dort suchen. Im Punkte–Bild liegen in Höhe v=1705 einige Punkte. Aus der Liste ergibt sich, dass $s1:=607$ und $s2:=725$ sein kann. Damit sind aus die Negativen dieser Werte Lösungen:

$s3=\mathrm{mod}(-s1,n) \blacktriangleright s3=1576$ $s4:=\mathrm{mod}(-s2,n) \blacktriangleright 1458$ Probe z.B. $\mathrm{mod}(s4^2,n) \blacktriangleright 1705$

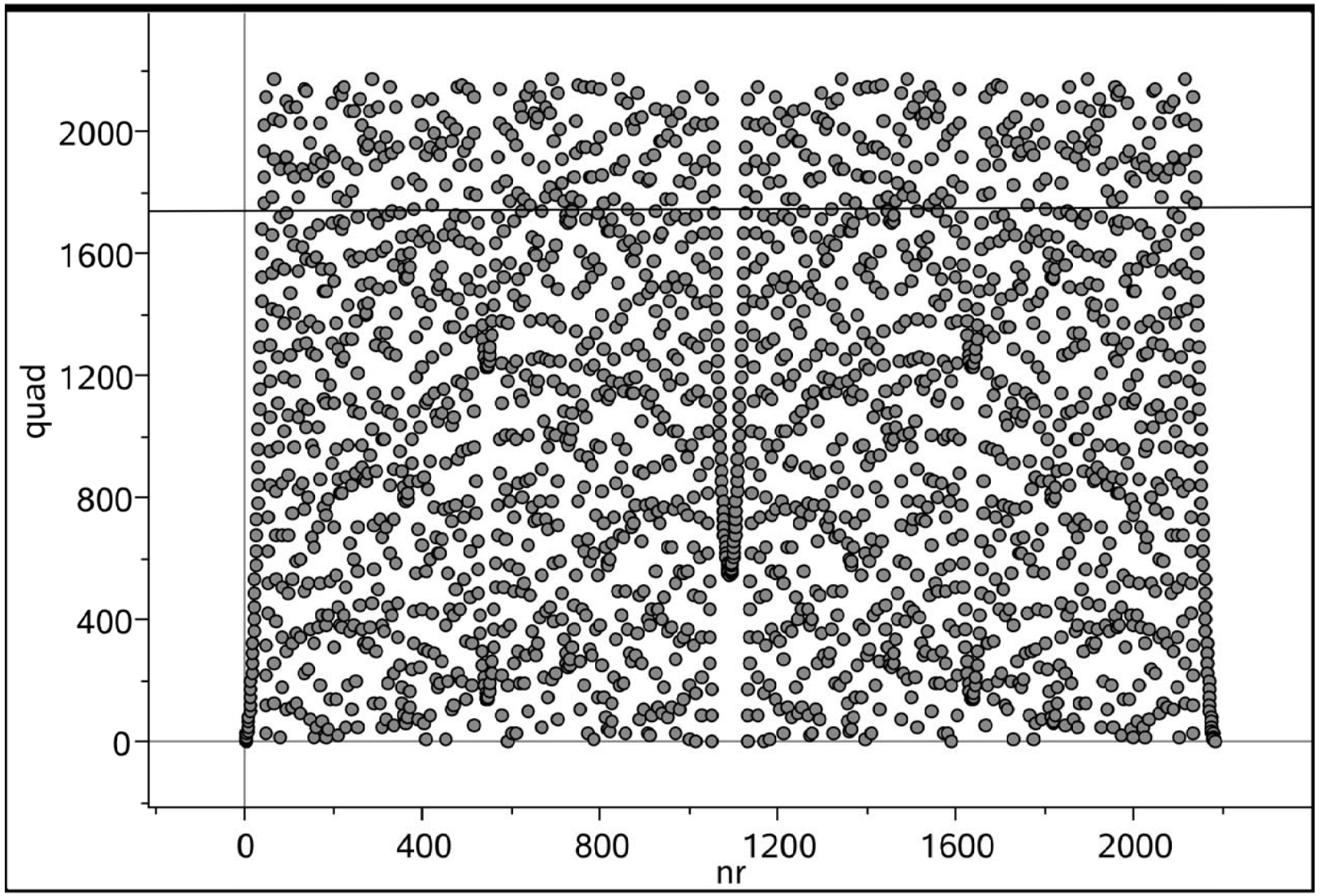
Für die Kryptografie ist dieser Betrugsversuch nicht erfolgreichversprechend, denn dieses Ergebnis kommt i.d.R mehrfach vor und man hat keine Chance bei echten Größenordnungender Kryptografie.

3.1

	A nr	B quad	C	D	E	F	G	H
◆	=seq(i,i,1,'	=mod(nr^2	=iffn(quad					
1	1	1	0					
2	2	4	0					
3	3	9	0					
4	4	16	0					
5	5	25	0					
6	6	36	0					
7	7	49	0					
8	8	64	0					
9	9	81	0					
10	10	100	0					
11	11	121	0					
12	12	144	0					
13	13	169	0					
14	14	196	0					
15	15	225	0					

A1 =1

3.2



3.3

	A bit	B lir	C lirq	D lisx_	E litest	F litestre	G	H
◆	=seq(rand	=seq(rand	=mod(lir^2,'	=mod(lirq*	=lirq	=mod(lisx_		
1	0	1219	358	358	358	358		
2	0	822	728	921	728	728		
3	0	1964	1701	2047	1701	1701		
4	0	599	2093	192	2093	2093		
5	1	932	248	248	248	248		
6	0	1980	271	271	271	271		
7	0	1494	2106	2106	2106	2106		
8	0	1010	1936	818	1936	1936		
9	0	324	182	182	182	182		
10	1	2066	736	1195	736	736		
11	1	1814	323	1785	323	323		
12	0	1141	400	400	400	400		
13	1	221	855	359	855	855		
14	0	1731	1554	1924	1554	1554		
15	1	1732	2025	46	2025	2025		

A1 =0

3.4

Besonderheiten, Erklärung für die Parabelform in der Mitte des Punktebildes

$ss:=\frac{n-1}{2} \rightarrow 1091 \quad vv:=\mathrm{mod}(ss^2,n) \rightarrow 546 \quad n \rightarrow 2183 \quad \sqrt{vv} \rightarrow \sqrt{546}$

$\mathrm{seq}(\mathrm{mod}((ss+i)^2,n),i,0,10) \rightarrow \{546,546,548,552,558,566,576,588,602,618,636\}$

$\mathrm{expand}\left(\left(\frac{nn-1}{2}+i\right)^2\right) \rightarrow i^2+i\cdot nn-i+\frac{nn^2}{4}-\frac{nn}{2}+\frac{1}{4} \quad \mathrm{factor}\left(i^2-i+\frac{1}{4}\right) \rightarrow \frac{(2\cdot i-1)^2}{4}$

$li:=\mathrm{seq}\left(\frac{(2\cdot i-1)^2}{4},i,0,10\right) \rightarrow \left\{\frac{1}{4},\frac{1}{4},\frac{9}{4},\frac{25}{4},\frac{49}{4},\frac{81}{4},\frac{121}{4},\frac{169}{4},\frac{225}{4},\frac{289}{4},\frac{361}{4}\right\}$

$\mathrm{mod}(kry\backslash ggte(4,n),n) \rightarrow [1 \quad 546 \quad 2182]$ Aha, das Inverse von 4 ist diese kleinste Zahl, anstelle des Viertels schreibe ich also *546

$lili:=\mathrm{seq}(\mathrm{mod}((2\cdot i-1)^2\cdot 546,n),i,0,15)$

$\rightarrow \{546,546,548,552,558,566,576,588,602,618,636,656,678,702,728,756\}$

und habe nun dieselbe Liste! Also gibt es in der Mitte die Parabelform.

Gleichung der Parabel $y=546\cdot(2(x-1091)-1)^2$

3.5

Angriffe, wenn b bekannt ist

Angriffe auf das Fiat–Shamir–Verfahren

Anton hat $n:=2183 \blacktriangleright 2183$ und $v:=1705 \blacktriangleright 1705$ bekanntgegeben.

2. Betrugsversuch von Mister X

Mister X übernimmt die gesamte Kommunikation mit n und v von Anton

Er berechnet mit dem Euklidischen Algorithmus das Inverse von v

$ea:=kry\backslash ggte(v,n) \blacktriangleright [1 \quad 580 \quad -453]$ $vinv:=mod(ea[1,2],n) \blacktriangleright 580$

$r:=randInt(10^{unt},n-2) \blacktriangleright 894$ $gcd(r,n) \blacktriangleright 1$ (1, anderenfalls neu!)

------ weiter nächste Seite ----------

Im Tabellenfenster ist alles hundertfach dargestellt.

Beweis der Durchführbarkeit: (alle Gleichungen modulo n)

$test:=y^2=r^2=r^2 \cdot vinv^b \cdot v=x\_ \cdot v^b=testre$

Daraus folgt: Keinesfalls darf Berta eine vorhersagbare Bitfolge wählen.

4.1

Wenn Mister X weiß, welches Bit b Berta senden wird, berechnet er ein anderes

$x\_:=\mathrm{mod}(r^2 \cdot vinv^b, n)$ ▸ 258, das er an Berta schickt.

2. Bertas Tat Berta empfängt x_ und sendet b=0 oder b=1 $b:=\mathrm{randint}(0,1)$ ▸ 0

3. Mister X's Reaktion empfängt b und antwortet mit y

$y:=\mathrm{mod}(r,n)$ ▸ 894

4. Bertas Test Berta quadriert y und erhält ihre Testzahl $test:=\mathrm{mod}(y^2,n)$ ▸ 258

Diese vergleicht sie mit x_ oder x_*v,

je nachdem sie b=0 oder b=1 gesendet hatte.

$erg:=\mathrm{ifFn}(b=0,\mathrm{ifFn}(test=x\_,\text{"ok"},\text{"Käse"}),\mathrm{ifFn}(test=\mathrm{mod}(x\_\cdot v,n),\text{"gut"},\text{"Quark"}))$

▸ ok

Hundertfache Ausführung im Tabellenfenster

4.2

	A bit	B lir	C lix_	D liy	E litest	F litestre	G	H
◆	=seq(rand	=seq(mod	=mod('li	=lir	=mod(liy^2	=mod(lix_		
1	0	1787	872	1160	872	872		
2	0	1300	638	1102	656	656		
3	1	1105	1740	1014	3	3		
4	1	1659	48	2084	1069	1069		
5	1	1319	1285	452	1285	1285		
6	1	1379	665	771	665	665		
7	1	733	1582	1313	1582	1582		
8	0	1131	749	1895	2173	2173		
9	1	2139	1029	2018	1029	1029		
10	0	539	28	1950	1897	1897		
11	1	493	1672	272	1945	1945		
12	0	2027	285	878	285	285		
13	0	20	1157	1904	1436	1436		
14	0	1811	1528	419	921	921		
15	0	1813	324	11	121	121		

A1 =0

4.3