

Fiat-shamir, 4-Stellig

Fiat-Shamir-Verfahren Haftendorn 2012, www.mathematik-verstehen.de
Vorbereitungsphase: zwei Primzahlen ($unt:=1 \cdot 1$, RandSeed 2503)
 $p:=\text{kry}\backslash\text{nextprime}(\text{randInt}(10^{unt}, 10^{unt+1})) \cdot 79$
 $q:=\text{kry}\backslash\text{nextprime}(\text{randInt}(10^{unt}, 10^{unt+1})) \cdot 73$
 $n:=p \cdot q \cdot 5767$
 $s:=\text{randInt}(10^{unt}, n-2) \cdot 1515 \quad \text{gcd}(s,n) \cdot 1$ (1, anderenfalls neu!)
 $v:=\text{mod}(s^2, n) \cdot 5726$
 Anton gibt $v \cdot 5726$ und $n \cdot 5767$ bekannt.

Anwendungsphase: 1. Anton's Tat: er wählt r teilerfremd zu n und berechnet x
 $r:=\text{randInt}(10^{unt}, n-2) \cdot 1062 \quad \text{gcd}(r,n) \cdot 1$ (1, anderenfalls neu!)
 $x:=\text{mod}(r^2, n) \cdot 3279$ Anton sendet x an Berta.

1.1

Anton hat $v \cdot 5726$ und $n \cdot 5767$ und $x \cdot 3279$ gesendet
2. Berta's Tat Berta empfängt x und sendet $b=0$ oder $b=1$ $b:=\text{randInt}(0,1) \cdot 1$
3. Anton's Reaktion empfängt x und antwortet mit y
 $y:=\text{ifFn}(b=0, r, \text{mod}(r, s, n)) \cdot 5704$
4. Berta's Test Berta quadriert y und erhält ihre Testzahl $\text{test}:=\text{mod}(y^2, n) \cdot 3969$
 Diese vergleicht sie mit x oder $x \cdot v$, je nachdem sie $b=0$ oder $b=1$ gesendet hatte.
 $\text{erg}:=\text{ifFn}(b=0, \text{ifFn}(\text{test}=x, "ok", "Käse"), \text{ifFn}(\text{test}=\text{mod}(x \cdot v, n), "gut", "Quark"))$
 $\cdot \text{gut}$
 In Kurzform $\text{test}=x \cdot v^b$. Nun wird das Verfahren m -mal hintereinander ausgeführt. Siehe Tabellenfenster. Die Wahrscheinlichkeit, dass Anton rein zufällig Erfolg hat, ist $\frac{1}{2^m} \cdot 2^m$, wird geprüft. **Beweis der Durchführbarkeit:**
 $\text{test}=y^2=(r \cdot s \cdot b)^2=r^2 \cdot s^{2b}=x \cdot (s^2)^b=x \cdot v^b \quad \text{q.e.d.}$

1.2

A	bit	B	lir	C	lix	D	liy	E	litest	F	litestre	
*	=seq	(rand	=seq	(rand	=mod	(lir^2	=mod	(lir*s	=mod	(liy^2	=mod	(lix^2
1	1	5400	2048	5400	2048	2048	2048					
2	1	2397	1677	2397	1677	1677	1677					
3	0	4952	1020	4952	1020	1020	1020					
4	1	977	2974	3803	4940	4940	4940					
5	0	5542	4489	5542	4489	4489	4489					
6	1	541	4331	701	1206	1206	1206					
7	0	2047	3367	4326	361	361	361					
8	0	5471	1111	1386	585	585	585					
9	1	1509	4883	2403	1642	1642	1642					
10	0	1823	1537	5219	420	420	420					
11	1	3411	2882	433	2945	2945	2945					
12	1	1490	5572	2453	2228	2228	2228					
13	0	3477	1897	3477	1897	1897	1897					
14	0	5064	4014	1850	2669	2669	2669					

1.3

Fiat-Shamir 12-stellig

Fiat-Shamir-Verfahren Haftendorn 2012
Vorbereitungsphase: zwei Primzahlen ($unt:=4 \cdot 4$, RandSeed 2503)
 $p:=\text{kry}\backslash\text{nextprime}(\text{randInt}(10^{unt}, 10^{unt+2})) \cdot 127997$
 $q:=\text{kry}\backslash\text{nextprime}(\text{randInt}(10^{unt}, 10^{unt+2})) \cdot 637097$
 $n:=p \cdot q \cdot 81546504709$
 $s:=\text{randInt}(10^{unt}, n-2) \cdot 17039309241 \quad \text{gcd}(s,n) \cdot 1$ (1, anderenfalls neu!)
 $v:=\text{mod}(s^2, n) \cdot 3634092279$
 Anton gibt $v \cdot 3634092279$ und $n \cdot 81546504709$ bekannt.

Anwendungsphase: 1. Anton's Tat: er wählt r teilerfremd zu n und berechnet x
 $r:=\text{randInt}(10^{unt}, n-2) \cdot 3273912618 \quad \text{gcd}(r,n) \cdot 1$ (1, anderenfalls neu!)
 $x:=\text{mod}(r^2, n) \cdot 19037350377$ Anton sendet x an Berta.

2.1

Anton hat $v \cdot 3634092279$ und $n \cdot 81546504709$ und $x \cdot 19037350377$ gesendet
2. Berta's Tat Berta empfängt x und sendet $b=0$ oder $b=1$ $b:=\text{randInt}(0,1) \cdot 0$
3. Anton's Reaktion empfängt b und antwortet mit y
 $y:=\text{mod}(r \cdot s^b, n) \cdot 3273912618$
4. Berta's Test Berta quadriert y und erhält ihre Testzahl
 $\text{test}:=\text{mod}(y^2, n) \cdot 19037350377$ Diese vergleicht sie mit $x \cdot v^b$.
 $\text{erg}:=\text{ifFn}(b=0, \text{ifFn}(\text{test}=x, "ok", "Käse"), \text{ifFn}(\text{test}=\text{mod}(x \cdot v, n), "gut", "Quark"))$
 $\cdot \text{ok}$
 Als Kurzform $\text{test}=x \cdot v^b \cdot \text{true}$
Beweis der Durchführbarkeit
 $\text{test}=y^2=(r \cdot s \cdot b)^2=r^2 \cdot s^{2b}=x \cdot (s^2)^b=x \cdot v^b \quad \text{q.e.d.}$

2.2

Angriffe, direkt

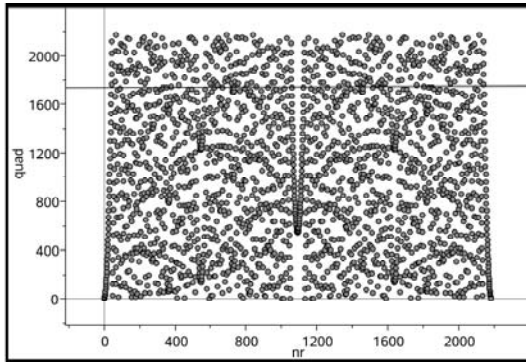
Angriffe auf das Fiat-Shamir-Verfahren
 Anton hat $n:=2183 \cdot 2183$ und $v:=1705 \cdot 1705$ bekanntgegeben.
 Um dies mit Punkten darzustellen, muss n unter 2500 liegen. Unter kann man dies ändern. Beim Neustart, sind es wieder andere Zahlen.

1. Betrugsversuch von Mister X, Geheimnis ausspähen
 $v=\text{mod}(s^2, n)$ 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:
 $s3=\text{mod}(s1, n) \cdot s3=1576 \quad s4=\text{mod}(s2, n) \cdot s4=1458$ Probe z.B.
 $\text{mod}(s4^2, n) \cdot 1705$ 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, 1,	=mod	(nr^2,	=ifFn	(quad			
1	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						

3.2



3.3

bit	lir	lirq	lix_x	litest	litestre
1	0	1219	358	358	358
2	0	822	728	921	728
3	0	1964	1701	2047	1701
4	0	599	2093	192	2093
5	1	932	248	248	248
6	0	1980	271	271	271
7	0	1494	2106	2106	2106
8	0	1010	1936	818	1936
9	0	324	182	182	182
10	1	2066	736	1195	736
11	1	1814	323	1785	323
12	0	1141	400	400	400
13	1	221	855	359	855
14	0	1731	1554	1924	1554

3.4

Besonderheiten, Erklärung für die Parabelform in der Mitte des Punktebildes

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

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

$$\text{expand}\left(\frac{(nm-1+i)^2}{2} \cdot i^2 + i \cdot nm - i + \frac{nm^2}{4} \cdot \frac{nm+1}{2} \cdot \text{factor}\left(i^2 - i + \frac{1}{4}\right) \cdot \frac{(2-i-1)^2}{4}\right)$$

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

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

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

$\cdot \{546, 546, 548, 552, 558, 566, 576, 588, 602, 618, 636, 656, 678, 702, 728, 756\}$
 und habe nun dieselbe Liste! Also gibt es in der Mitte die Parabelform.

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

3.5

Angriffe, wenn b bekannt ist

Angriffe auf das Fiat-Shamir-Verfahren

Anton hat $n := 2183 \cdot 2183$ und $v := 1705 \cdot 1705$ 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

$$ea := \text{kry}(\text{ggte}(v, n) \cdot [1 \ 580 \ -453]) \quad \text{vinv} := \text{mod}(ea[1,2], n) \cdot 580$$

$$r := \text{randInt}(10^{\text{uint}(n-2)} \cdot 894 \quad \text{gcd}(r, n) \cdot 1 \quad (1, \text{anderfalls neu!})$$

----- weiter nächste Seite -----

Im Tabellenfenster ist alles hundertfach dargestellt.

Beweis der Durchführbarkeit: (alle Gleichungen modulo n)

$$\text{test} := y^2 = r^2 = r^2 \cdot \text{vinv} \cdot v = x \cdot v = \text{testre}$$

4.1

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

$$x_ := \text{mod}(r^2 \cdot \text{vinv} \cdot b, n) \cdot 258,$$

das er an Berta schickt.

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

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

$$y := \text{mod}(r, n) \cdot 894$$

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

Diese vergleicht sie mit $x_$ oder $x_ \cdot v$,

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

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

$\cdot \text{ok}$

Hundertfache Ausführung im Tabellenfenster

4.2

bit	lir	lix_x	liy	itest	litestre
1	0	1160	872	1160	872
2	0	1102	638	1102	656
3	1	1014	1740	1014	3
4	1	2084	48	2084	1069
5	1	452	1285	452	1285
6	1	771	665	771	665
7	1	1313	1582	1313	1582
8	0	1895	749	1895	2173
9	1	2018	1029	2018	1029
10	0	1950	28	1950	1897
11	1	272	1672	272	1945
12	0	878	285	878	285
13	0	1904	1157	1904	1436
14	0	419	1528	419	921

4.3