Small primitive roots and malleability of RSA moduli

Jorge J. Urroz and Luis Dieulefait, UPC and UB, Barcelona

Castro Urdiales, July 9, 2012

Problem. (Malleability of Factoring) Given and RSA modul n find another integer n' coprime to n so that the factorization of n' will help to factorize n.

Problem. (Malleability of Factoring) Given and RSA modul n find another integer n' coprime to n so that the factorization of n' will help to factorize n.

Inspired by P. Pailler and J. Villar.: OW equivalent to factoring and resisting CCA are incompatible goals for sigle-key cryptosystems.

Problem. (Malleability of Factoring) Given and RSA modul n find another integer n' coprime to n so that the factorization of n' will help to factorize n.

Inspired by P. Pailler and J. Villar.: OW equivalent to factoring and resisting CCA are incompatible goals for sigle-key cryptosystems.

There is no instantiation of some simple RO-model schemes (Rabin) in the standard model which CCA security is equivalent to factoring via key-preserving reductions. From key preserving reductions to arbitrary reductions need non-malleability

Conjecture. Factoring is not malleable.

Conjecture. Factoring is not malleable.

Theorem. Given any $n = pq$ RSA modul there exist another integer n' so that factoring n' allow us to factor n in polynomial time.

Conjecture. Factoring is not malleable.

Theorem. Given any $n = pq$ RSA modul there exist another integer n' so that factoring n' allow us to factor n in polynomial time.

$n' = 2^n - 1$

A particular case

Theorem (L. Dieulefait and J. Jiménez Urroz)

Let $n = pq$ $z < p, q < 2z$, be and RSA modulus such that either we have $2^{p-1} \not\equiv 1 \pmod{q}$ or $2^{q-1} \not\equiv 1 \pmod{p}$ and let $n' = 2^n - 1$. Then, with the factorization of n' we can find a prime divisor of n in polynomial time.

A particular case

Theorem (L. Dieulefait and J. Jiménez Urroz)

Let $n = pq$ $z < p, q < 2z$, be and RSA modulus such that either we have $2^{p-1} \not\equiv 1 \pmod{q}$ or $2^{q-1} \not\equiv 1 \pmod{p}$ and let $n' = 2^n - 1$. Then, with the factorization of n' we can find a prime divisor of n in polynomial time.

Proof To factor n we use an oracle $\mathcal{O}$ that allow us to factor any given n‘ coprime to n. Let $S = \{r \pmod{n} \neq 1, r | n', \text{ prime}\}$

A particular case

Theorem (L. Dieulefait and J. Jiménez Urroz)

Let $n = pq$ $z < p, q < 2z$, be and RSA modulus such that either we have $2^{p-1} \not\equiv 1 \pmod{q}$ or $2^{q-1} \not\equiv 1 \pmod{p}$ and let $n' = 2^n - 1$. Then, with the factorization of n' we can find a prime divisor of n in polynomial time.

Proof To factor n we use an oracle $\mathcal{O}$ that allow us to factor any given n‘ coprime to n. Let $S = \{r \pmod{n} \neq 1, r | n', \text{ prime}\}$

Algorithm.

- Send n' in binary form to $\mathcal{O}$.
- Take $r \in S$ and compute $(r - 1, n) = p$.

Step 1. There exist such r. Indeed if every prime of $2^n - 1$ is 1 modulo n then $2^n - 1 \equiv 1 \pmod{n}$ or $2^{n-1} \equiv 1 \pmod{n}$

$$2^{n-1} \equiv 1 \pmod{p}, \text{ and } 2^{n-1} \equiv 1 \pmod{q}$$

But

$$2^{n-1} = 2^{(p-1)q+q-1} \equiv 2^{q-1} \pmod{p}$$

So,

$$2^{q-1} \equiv 1 \pmod{p}, \text{ and } 2^{p-1} \equiv 1 \pmod{q}$$

Step 1. There exist such r. Indeed if every prime of $2^n - 1$ is 1 modulo n then $2^n - 1 \equiv 1 \pmod{n}$ or $2^{n-1} \equiv 1 \pmod{n}$

$$2^{n-1} \equiv 1 \pmod{p}, \text{ and } 2^{n-1} \equiv 1 \pmod{q}$$

But

$$2^{n-1} = 2^{(p-1)q+q-1} \equiv 2^{q-1} \pmod{p}$$

So,

$$2^{q-1} \equiv 1 \pmod{p}, \text{ and } 2^{p-1} \equiv 1 \pmod{q}$$

Step 2. $2^n \equiv 1 \pmod{r}$ and $2^{r-1} \equiv 1 \pmod{r}$ Hence

$$2^{(n,r-1)} \equiv 1 \pmod{r}$$

and $(n, r-1) \neq 1, n$. Note that $(n, r-1) = (n, r \pmod{n} - 1)$

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

The previous algorithm does not work for pseudoprime modulus.

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

The previous algorithm does not work for pseudoprime modulus.

Are there infinitely many pseudoprimes?

Pseudoprimes

Definition. An integer n so that $2^n - 1 \equiv 1 \pmod{n}$ is called a pseudoprime.

The previous algorithm does not work for pseudoprime modulus.

Are there infinitely many pseudoprimes?

Theorem. (Alford, Granville, Pomerance) There are infinitely mane Charmichael numbers.

A Charmichael number is a composite number n such that $b^{n-1} \equiv 1 \pmod{n}$ for all $(b, n)) = 1$. Exemple $561 = 3 \cdot 11 \cdot 17$.

Theorem. (Pomerance) Given $x > 0$, the number of pseudoprimes up to x is less than

$$x \exp(-\frac{1}{2} \log x \log \log \log x / \log \log x)$$

Proposition For large z, the number of RSA moduli $n = pq$, $z < p, q < 2z$ pseudoprimes are less than

$$\left(\frac{z}{\log z}\right)^2 \frac{(\log \log \log z)^2}{\log z}$$

Proof.
$2^{(p-1,q-1)} \equiv 1 \pmod{n}$ not possible if $(p-1, q-1) < \log z$. Let $\pi(d, z) = |\{p \equiv 1 \pmod{d}, z < p < 2z\text{prime}\}|$.

$$\sum_{\substack{z<p,q<2z \\ (p-1,q-1)>\log z}} 1 = \sum_{\log z<d<z} \pi(d,z)^2 \sim \sum_{\log z<d<z} \left(\frac{z}{\varphi(d)\log z}\right)^2$$

Since

$$\varphi(d) = d\prod_{p|d}\left(1-\frac{1}{p}\right) > d\prod_{p<\log d}\left(1-\frac{1}{p}\right) > \frac{Cd}{\log\log d}$$

$$\sum_{\log z<d<z} \frac{1}{\varphi(d)^2} < c\sum_{\log z<d<z} \frac{\log\log d}{d^2} < \frac{c(\log\log\log z)^2}{\log z}.$$

Theorem. (Barban-Davenport-Halberstam)

$$\sum_{d \le z^{1-\varepsilon}} \left| \psi(d,z) - \frac{z}{\varphi(d)} \right|^2 \ll \frac{z^2}{(\log z)^A},$$

with a constant depending only in ε and A.

Primitive roots and the general case.

To avoid the pseudoprime moduli, we will choose another integer m and $n' = m^n - 1$ with a prime factor not 1 modulo n.

Primitive roots and the general case.

To avoid the pseudoprime moduli, we will choose another integer m and $n' = m^n - 1$ with a prime factor not 1 modulo n.

Definition. Given a prime p, a primitive root modulo p is an integer so that $< m >= \mathbb{F}_p^*$. $m^d \not\equiv 1 \pmod{p}$ for any $d < p - 1$.

Primitive roots and the general case.

To avoid the pseudoprime moduli, we will choose another integer m and $n' = m^n - 1$ with a prime factor not 1 modulo n.

Definition. Given a prime p, a primitive root modulo p is an integer so that $< m >= \mathbb{F}_p^*$. $m^d \not\equiv 1 \pmod{p}$ for any $d < p - 1$.

If $n = pq$, $q < p$ and m is a primitive root modulo p, $m^{n-1} \not\equiv 1 \pmod{n}$, since $m^{q-1} \not\equiv 1 \pmod{p}$.

Question. How difficult is to find a primitive root modulo p without knowing p?.

There are $\varphi(p-1)$ primitive roots modulo p. Hence the probability to find one is

$$\frac{\varphi(p-1)}{p-1} = \prod_{q|p-1}\left(1-\frac{1}{q}\right) > \prod_{q<\log p}\left(1-\frac{1}{q}\right) > \frac{c}{\log\log p}.$$

Question. How difficult is to find a primitive root modulo p without knowing p?.

There are $\varphi(p-1)$ primitive roots modulo p. Hence the probability to find one is

$$\frac{\varphi(p-1)}{p-1} = \prod_{q|p-1}\left(1-\frac{1}{q}\right) > \prod_{q<\log p}\left(1-\frac{1}{q}\right) > \frac{c}{\log\log p}.$$

In particular a random set of size $C\log\log p$ should have positive probability to contain a primitive root modulo p. Since $p < n$ a set of size $C\log\log n$ should have positive probability to contain a primitive root modulo p. The probability for a set of this size to contain no primitive roots is

$$\left(1-\frac{c}{\log\log p}\right)^{C\log\log p} \sim e^{-Cc}.$$

Results.

(E. Bach) Let $g(p)$ the least primitive root modulo p.

$$g(p) \leq e^{\gamma} \log p (\log \log p)^2 (1 + \varepsilon).$$

Results.
(E. Bach) Let $g(p)$ the least primitive root modulo p.

$$g(p) \leq e^{\gamma} \log p (\log \log p)^2 (1 + \varepsilon).$$

Theorem (V. Shoup) Under GRH, $g(p) \ll (\log p)^6$

Results.
(E. Bach) Let $g(p)$ the least primitive root modulo p.

$$g(p) \leq e^{\gamma} \log p (\log \log p)^2 (1 + \varepsilon).$$

Theorem (V. Shoup) Under GRH, $g(p) \ll (\log p)^6$

Conjecture (Artin) Any given integer a not $1, -1$ or a perfect square is a primitive root for a positive proportion of primes $\prod_q \left(1 - \frac{1}{q(q-1)}\right) \sim 0.37395$.

Results.
(E. Bach) Let $g(p)$ the least primitive root modulo p.

$$g(p) \leq e^{\gamma} \log p (\log \log p)^2 (1 + \varepsilon).$$

Theorem (V. Shoup) Under GRH, $g(p) \ll (\log p)^6$

Conjecture (Artin) Any given integer a not $1, -1$ or a perfect square is a primitive root for a positive proportion of primes $\prod_q \left(1 - \frac{1}{q(q-1)}\right) \sim 0.37395$.

Heath-Brown Among $3, 5, 7$ there is a primitive root for infinitely many p

For each integer m set $n'_m = (m^n - 1)/(m - 1)$, and $S_m = \{r \pmod{n} \neq 1 : r \text{ prime } r | n'_m\}$.

For each integer m set $n'_m = (m^n - 1)/(m - 1)$, and $S_m = \{r \pmod{n} \neq 1 : r \text{ prime } r | n'_m\}$.

Algorithm The m-ary representation of n is c independent of m

- m=2
- Send (c, m) to $\mathcal{O}$
- $S =$, $m = m + 1$. Return
- take $r \in S$ and compute $d = (r - 1, n)$.

For each integer m set $n'_m = (m^n - 1)/(m - 1)$, and $S_m = \{r \pmod{n} \neq 1 : r \text{ prime } r | n'_m\}$.

Algorithm The m-ary representation of n is c independent of m

- m=2
- Send (c, m) to $\mathcal{O}$
- $S =$, $m = m + 1$. Return
- take $r \in S$ and compute $d = (r - 1, n)$.

Theorem (L. Dieulefait and J. Jiménez Urroz)

Let $n = pq$ $z < p, q < 2z$, be and RSA modulus . Then, under GRH the previous algorithm gives a prime divisor of n in polynomial time.

Proof

Lemma Let $n = pq$ and RSA modulus and m such that $(m-1, n) = 1$. Then $(n'_m, m-1) = 1$. If $r|(n'_m, m-1)$, then $n'_m = \sum_{j=0}^{n-1} m^j \equiv n \pmod{r}$.

Step 1. There exist such r. Indeed if every prime of n'_m is 1 modulo n then $m'_n \equiv 1 \pmod{n}$ or $m^{n-1} \equiv 1 \pmod{n}$

$$m^{n-1} \equiv 1 \pmod{p}, \text{ and } m^{n-1} \equiv 1 \pmod{q}$$

But

$$m^{n-1} = 2^{(p-1)q+q-1} \equiv m^{q-1} \pmod{p}$$

which is not possible.

Proof

Lemma Let $n = pq$ and RSA modulus and m such that $(m-1, n) = 1$. Then $(n'_m, m-1) = 1$. If $r|(n'_m, m-1)$, then $n'_m = \sum_{j=0}^{n-1} m^j \equiv n \pmod{r}$.

Step 1. There exist such r. Indeed if every prime of n'_m is 1 modulo n then $m'_n \equiv 1 \pmod{n}$ or $m^{n-1} \equiv 1 \pmod{n}$

$$m^{n-1} \equiv 1 \pmod{p}, \text{ and } m^{n-1} \equiv 1 \pmod{q}$$

But

$$m^{n-1} = 2^{(p-1)q+q-1} \equiv m^{q-1} \pmod{p}$$

which is not possible.

Step 2. $m^n \equiv 1 \pmod{r}$ and $m^{r-1} \equiv 1 \pmod{r}$. Hence

$$m^{(n,r-1)} \equiv 1 \pmod{r}$$

and $(n, r-1) \neq 1, n$. Note that $(n, r-1) = (n, r \pmod{n} - 1)$