Trapdoor-Free RSA Like Assumption

Yvo Desmedt
BT Chair of Information Security
University College London, UK

August 23, 2006

Extended Abstract

Although a lot of research was done in the 1980's on proving cryptosystems based on factoring, two examples being Rabin's scheme and Goldwasser-Micali-Rivest, in the last decade a very large number of papers have appeared using the Diffie-Hellman assumptions and variants.

We make two remarks on this approach. First the Diffie-Hellman assumptions may be wrong, while the factoring one may be correct. Second, the Diffie-Hellman assumption does not involve a trapdoor, but both factoring as well as RSA do. For obvious reasons it may be good to obtain a variant of the RSA assumption, for which we can give reasonable evidence that it is likely trapdoor free.

We now propose a first proposal. Assume that a party chooses $n = pq$ and chooses some uniformly random odd e between 1 and n. Instead of using the function $f_1(r) := r^e \bmod n_1$ only (as in the ordinary RSA), users additionally output $f_2(r) := r^{e_2} \bmod n_2$, where $n_2 = n_1 + d$, where d is small and $e_2 = e$. We now discuss how to use f_1 and f_2 to propose a probabilistic one-way function. Assume (n_1, n_2, e) is public. Let $x \in Z^*_{n_1}$ be an input. The user first chooses $r_1 \in_R Z_n$ computes $r_2 = x - r_1 \bmod n_2$ and outputs $f(x) = (f_1(r_1), f_2(r_2))$. Observe that r_2 is statistically indistinguishable from a uniform random element in Z_{n_2}, as follows easily from [**?**]. We now wonder whether this probabilistic function f is trapdoor-free. It is trivial to see that this corresponds to analyzing whether anybody can construct an n_1 and n_2 such that he/she can computationally invert f_1 and f_2.

We now analyze the security of this first proposal. Assume $q > p$ and $q = p + \alpha$. We now analyze whether a party can choose p, q, p' and q', where p and q are primes, but p' and q' are not necessarily. Let $p' = p + a$ and $q' = q + b$. The condition $p'q' = n + d$ now gives us $(p+a)(q+b) = pq + bp + aq + ab = pq + d$ which is true if and only if $bp + a(p + \alpha) + ab = d$, or

$$p(b + a) + \alpha a + ab = d. \qquad (1)$$

If we want to demonstrate that the first proposal is insecure, then necessary conditions are sufficient. Since p is large, a and b are small and α (relatively) small, we decide to choose $b = -a$. Using this choice, Eq. 1 becomes:

$$a^2 - \alpha a + d = 0 \tag{2}$$

Solving this equation in the unknown a we obtain:

$$a = \frac{\alpha \pm \sqrt{\alpha^2 - 4d}}{2} \tag{3}$$

Since α is even, we can replace it by $2k$. Then Eq. 3 becomes:

$$a = k \pm \sqrt{k^2 - d} \tag{4}$$

We now use Eq. 4 to demonstrate that the first proposal is insecure. Take $\alpha = 2$, i.e. $k = 1$, which means we speak about twin primes p and q. Moreover, we let $d = 1$. Then $a = 1$ and $b = -1$. Obviously $n + 1$ becomes a square number. So, if p and q are reasonable sized primes, then the one who constructs n might be able to factor $n + d$ and then f_2 can be inverted in polynomial time.

We now discuss a second proposal. Instead of using just two moduli, being n_1 and $n_2 = n_1 + d$, we will use several. We let $n_i = n_1 + d_i$, where all d_i are small, and this for $i = 2, \ldots, l$. We conjecture that when l is not too small, there will be at least one function $f_i(r) := r^{e_i} \bmod n_i$ which one cannot invert in polynomial time. A possible choice for e_i is $e_i = e_1$. We do not require that $\gcd(e_i, \phi(n_i)) = 1$. The probabilistic function f applied on x now corresponds to choose r_i such that $r_1 + r_2 + \cdots + r_l = x \bmod n_1$, then f_i is applied on r_i, so $f(x) = (f_1(r_1), f_2(r_2), \ldots, f_l(x_l))$.