Cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

10 Assignment: Security Reductions and r-safe moduli

(Due: Thursday, 28 January 2010, 23^{59})

You have encountered several levels of security:

- Unbreakability,
- Universal Unforgeability,
- Existential Unforgeability (EUF);

along with different means for an attacker:

- Key-Only Attack,
- Non-adaptive Chosen Message Attack,
- Chosen Message Attack (CMA).

Pairing an adversarial goal with an attack model defines a security notion, e.g. EUF-CMA.

Exercise 10.1. Security notions (4 points)

Consider the ElGamal signature scheme. Assume that the DL is hard and decide for each of the 9 security notions whether the scheme is

- secure,
- not secure
- or the answer is unknown.

What can you say, if you assume that DL is easy? Use the connections between the security notions to simplify your argument.

Exercise 10.2 (Security reduction)**.** (3 points) For a signature scheme, a message is first hashed and then the hash value is signed. Assume that the signature scheme is secure in the EUF-CMA model. Does that imply that the hash function is collision resistant? Prove your answer.

Exercise 10.3 (Generating r-safe RSA moduli)**.** (5 points) An example for an r-safe modulus pq is given by SOPHIE-GERMAIN primes $p = 2u+1$, where $u > r$ is also prime, and similarly for q. It is conjectured, but not proven, that there are infinitely many SOPHIE-GERMAIN primes.

(i) Write a small program that picks on input r and x random integers $a \leq x$ until a is a Sophie-Germain prime $2u + 1$ with $u > r$. Run your program for $r = 2^{10}$, $x = 2^{60}$ several times to get a good estimate for the expected number of picks.

Repeat the experiment with increasing x, say by factors of 2, to get an idea for the behaviour as x increases. Compare the behaviour to $x/\log^2 x$.

(ii) Modify your program to find primes p where $(p-1)/2$ has no prime factor smaller than r. How many loops do you observe on average for $r = 2^{10}$ and $x = 2^{60}$?

As above, study the behaviour for increasing x and compare it to $x/\log^2 x$.