Advanced Cryptography: Algorithmic Cryptanalysis

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

7. Exercise sheet
Hand in solutions until Saturday, 28 May 2011, 23:59h.

To estimate the average effort you put into solving the following exercises, please add after each exercise the amount of time you spent for it.

Exercise 7.1 (hashing with permutations). (9 points)

Consider a hash function obtained by directly applying the Merkle-Damgård construction (without appending an extra block which encodes the message length) to family of *permutations* π_m. This means that starting from an intermediate hash value h_i and a message block m_i, the next hash value is $h_{i+1} = \pi_{m_i}(h_i)$. The goal of this exercise is to show a weakness of this hash function with respect to the preimage property.

(i) Show that when π_m^{-1} is available for every m, preimages can be easily computed if you can choose the initialization vector h_0 at your digression. [2]

This is also true, if h_0 is a fixed value. Consider the following strategy.

- Choose a long sequence of message blocks M_i and compute, starting from h_0, the intermediate hash value which we denote by h_i.
- Let h_F be the hash value for which you want to compute a preimage. Choose another long sequence of message blocks M_i' and compute *backwards*, starting from h_F, the intermediate hash values h_i' leading to h_F with the blocks M_i'.
- Stop when h_i' appears in the list of h_i's from step Exercise 7.1.

(ii) How does the strategy above lead to a preimage for h_F. [2]

(iii) Let π_m be a n-bit block cipher with n-bit keys. What is a reasonable choice for the number of blocks in step Exercise 7.1? How many blocks do you expect to process in step Exercise 7.1 until the condition Exercise 7.1 is satisfied. Compare this to the generic complexity of a brute-force preimage finder. [5]

Exercise 7.2 (adding non-linearity to the linear model of SHA-0).

(8+4 points)

In the lecture we found 63 non-zero bit sequences of 80 bits that can be used to introduce local collisions in a way that is consistent with the message expansion. Our goal is the maximize the probability of success that such a bit sequence will also yield a collision for the original SHA-0.

We

- choose a bit sequence of small weight, and
- insert it at bit position 1.

2 (i) Justify the two criteria. (Remember that bit positions are numbered from 0 to 31.)

Let us track the insertion of a local collision on bit 1 of $W^{(i)}$. For simplicity, assume that the perturbation is $\uparrow$. This affects bit 1 of $A^{(i+1)}$.

If no unwanted carries occur, bit 1 of $A^{(i+1)}$ is also $\uparrow$ and all other remain unchanged. Otherwise, bit 1 of $A^{(i+1)}$ is $\downarrow$ and bit 2 is no longer constant and this may propagate.

1 (ii) Assume the inputs of the addition are uniformly random values. What is the probability that no carry occurs?

In step $i+2$, the change $\uparrow$ in $A^{(i+1)}$ is invoked (after rotation) in the computation of $A^{(i+2)}$. This is corrected by the change in $W^{(i+2)}$.

1 (iii) Give a necessary and sufficient condition for the change in bit 6 of $W^{(i+2)}$ such that the correction is performed correctly, i.e. as in the linear model.

In step $i+3$, the change $\uparrow$ is on bit 1 of $B^{(i+2)}$ and involved in the computation of $A^{(i+3)}$. It is corrected with bit 1 of $W^{(i+3)}$. Three cases are possible, after $B^{(i+2)}$ is processed by f (XOR, MAJ, or IF):

- The change $\uparrow$ has vanished,
- the change $\uparrow$ remains unchanged, or
- the change $\uparrow$ has been reversed to a change $\downarrow$

3 (iv) Compute the probability that a change does not vanish for each of the three possible functions.

The next corrections concern bit 31 of $A^{(i+4)}$ and $A^{(i+5)}$.

(v) Show that these corrections are always done correctly, if the perturbation does not vanish. In other words, they are done correctly if the change remains unchanged or if the change is reversed. 1

Finally, the correction on bit 31 of $A^{(i+6)}$ is always correctly canceled by the correction on bit 31 of $W^{(i+5)}$ and we can compute for any round i the probability of successfully applying a single local collision at position 1 in this round.

(vi) Assume that these probabilities have been computed. Describe a (feasible) strategy to produce collisions from that information. +4

Exercise 7.3 (Lattices and the gcd). (4 points)

Let $a, b \in \mathbb{N}_{>0}$ and consider the lattice $L = a\mathbb{Z} + b\mathbb{Z}$ spanned by the vectors (a) and (b).

(i) Show that $L = \gcd(a, b)\mathbb{Z}$. Hint: Extended Euclidean Algorithm! 3

(ii) Conclude that a shortest vector in L has length $\gcd(a, b)$. 1

Exercise 7.4 (Transforming bases). (5+5 points)

Let $B \in \mathbb{R}^{\ell \times n}$ be a basis of the lattice L, this is the lattice L is generated by the rows $b_1, \ldots, b_\ell \in \mathbb{R}^n$ of B. Express each of the following matrix operations on B as a left multiplication by a unimodular matrix $U \in \mathbb{R}^{\ell \times \ell}$, i.e. an integer matrix with $\det(U) = \pm 1$:

(i) Swap the order of the rows of B, 2

(ii) Multiply a row by -1, 1

(iii) Add an integer multiple of a row to another row, i.e. set $b_i \leftarrow b_i + ab_j$ where $i \neq j$ and $a \in \mathbb{Z}$. 2

(iv) Show that any unimodular matrix can be expressed as a sequence of these three elementary integer row transformations. +5