Subject: A new attack on DES

Research announcement: A new cryptanalytic attack on DES

Eli Biham Adi Shamir

Computer Science Dept. Applied Math Dept.
The Technion The Weizmann Institute
Israel Israel

October 18, 1996

(DRAFT)

In September 96, Boneh Demillo and Lipton from Bellcore announced an ingenious new type of cryptanalytic attack which received widespread attention (see, e.g., John Markoff's 9/26/96 article in the New York Times). Their full paper had not been published so far, but Bellcore's press release and the authors' FAQ (available at http://www.bellcore.com/PRESS/ADVSRY96/medadv.html) specifically state that the attack is applicable only to public key cryptosystems
such as RSA, and not to secret key algorithms such as the Data Encryption Standard (DES). According to Boneh, "The algorithm that we apply to the device's faulty computations works against the algebraic structure used in public key cryptography, and another algorithm will have to be devised to work against the nonalgebraic operations that are used in secret key techniques." In particular, the original Bellcore attack is based on specific algebraic properties of modular arithmetic, and cannot handle the complex bit manipulations which underly most secret key algorithms.

In this research announcement, we describe a related attack (which we call Differential Fault Analysis, or DFA), and show that it is applicable to almost any secret key cryptosystem proposed so far in the open literature. In particular, we have actually implemented DFA in the case of DES, and demonstrated that under the same hardware fault model used by the Bellcore researchers, we can extract the full DES key from a sealed tamperproof DES encryptor by analysing fewer than 200 ciphertexts generated from unknown cleartexts. The power of Differential Fault Analysis is demonstrated by the fact that even if DES is replaced by triple DES (whose 168 bits of key were assumed to make it practically invulnerable), essentially the same attack can break it with essentially the same number of given ciphertexts.

We would like to greatfully acknowledge the pioneering contribution of Boneh Demillo and Lipton, whose ideas were the starting point of our new attack.

In the rest of this research announcement, we provide a short technical summary of our practical implementation of Differential Fault Analysis of DES. Similar attacks against a large number of other secret key cryptosystems will be described in the full version of our paper.

TECHNICAL DETAILS OF THE ATTACK

The attack follows the Bellcore fundamental assumption that by exposing a sealed tamperproof device such as a smart card to certain physical effects (e.g., ionizing or microwave radiation), one can induce with reasonable probability a fault at a random bit location in one of the registers at some random intermediate stage in the cryptographic computation. Both the bit location and the round number are unknown to the attacker.

We further assume that the attacker is in physical possesion of the tamperproofdevice, so that he can repeat the experiment with the same cleartext and key but without applying the external physical effects. As a result, he obtains two ciphertexts derived from the same (unknown) cleartext and key, where one of the ciphertexts is correct and the other is the result of a computation corrupted by a single bit error during the computation. For the sake of simplicity, we assume that one bit of the right half of the data in one of the 16 rounds of DES is flipped from 0 to 1 or vice versa, and that both the bit position and the round number are uniformly distributed.

In the first step of the attack we identify the round in which the fault occurred. This identification is very simple and effective: If the fault occurred in the right half of round 16, then only one bit in the right half of the ciphertext (before the final permutation) differs between the two ciphertexts. The left half of the ciphertext can differ only in output bits of the S box (or two S boxes) to which this single bit enters, and the difference must be

related to non-zero entries in the difference distribution tables of these S boxes. In such a case, we can guess the six key bit of each such S box in the last round, and discard any value which disagree with the expected differences of these S boxes (e.g., differential cryptanalysis). On average, about four possible 6-bit values of the key remain for each active S box.

If the faults occur in round 15, we can gain information on the key bits entering more than two S boxes in the last round: the difference of the right half of the ciphertext equals the output difference of the F function of round 15. We guess the single bit fault in round 15, and verify whether it can cause the expected output difference, and also verify whether the difference of the right half of the ciphertext can cause the expected difference in the output of the F function in the last round (e.g., the difference of the left half of the ciphertext XOR the fault). If successful, we can discard possible key values in the last round, according to the expected differences. We can also analyse the faults in the 14'th round in a similar way. We use counting methods in order to find the key. In this case, we count for each S box separately, and increase the counter by one for any pair which suggest the six-bit key value by at least one of its possible faults in either the 14'th, 15'th, or 16'th round.

We have implemented this attack on a personal computer. Our analysis program found the whole last subkey given less than 200 ciphertexts, with random single-faults in all the rounds.

This attack finds the last subkey. Once this subkey is known, we can proceed in two ways: We can use the fact that this subkey contains 48 out of the 56 key bits in order to guess the missing 8 bits in all the possible 2^8=256 ways. Alternatively, we can use our knowledge of the last subkey to peel up the last round (and remove faults that we already identified), and analyse the preceding rounds with the same data using the same attack. This latter approach makes it possible to attack triple DES (with 168 bit keys), or DES with independent subkeys (with 768 bit keys).

This attack still works even with more general assumptions on the fault locations, such as faults inside the function F, or even faults in the key scheduling algorithm. We also expect that faults in round 13 (or even prior to round 13) might be useful for the analysis, thus reducing the number of required ciphertext for the full analysis.

OTHER VULNERABLE CIPHERS

Differential Fault Analysis can break many additional secret key cryptosystems, including IDEA, RC5 and Feal. Some ciphers, such as Khufu, Khafre and Blowfish compute their S boxes from the key material. In such ciphers, it may be even possible to extract the S boxes themselves, and the keys, using the techniques of Differential Fault Analysis. Differential Fault Analysis can also be applied against stream ciphers, but the implementation might differ by some technical details from the implementation described above.