Strengthening Cryptosystems by Re-Keying

John Black

February 9, 1999

1 Introduction

In light of the disturbing efficacy of the recently-discovered deletion attack of Knudsen and Mirza [2], we propose a subtle strengthening procedure to avoid their method. We call our approach "strengthening by re-keying."

The basic technique employed is called the "PUT IT BACK" algorithm. The fundamental idea here is this: when Knudsen and Mirza delete the key, we put it back. Details follow.

2 One-Time Pad Revitalized

The well-known one-time pad [3] was devestated by [2], but fortunately the intellectual gold-mine that *is* U.C. Davis has come to the rescue.

Normally we are given plaintext P and a secret key K such that $n = |P| = |K|$. Then we produce an encryption of P by computing $C = P + K$ in the finite field $\mathrm{GF}(2^n)$. (Note that this can be done *without* the generation of irreducible polynomials! See [1].)

Now [2] uses the following clever attack: they set $K = 0$. (The alert reader will note that their attack is phrased somewhat differently, but the effect is the same.) Now we have $C = P$, which leaks information about the plaintext.

We propose the following fix: PUT IT BACK again! Explicitly, we set K back to its original value and compute $C = P + K$ again. This admittedly ingenious method now revives all the security promised by [3].

3 Iterated Attacks

Of course we must worry about repeated applications of the deletion attack. The obvious question arises: what if K is set back to 0 again. Well, again we have devised an ingenious remedy: we PUT IT BACK again.

Theorem 3.1 *No matter how many times they delete it, we can always PUT IT BACK.*

Proof: Assume the deletion method is applied n times. The proof is by induction on n: for $n = 1$, we clearly just PUT IT BACK (see Section 2). Now assuming the key has been deleted and put back n times, we see that deleting it $n+1$ times requires we put it back only *one further time* (i.e., the method is efficient). ∎

4 Acknowledgements

The author was supported by an NSF grant whose number he'd better not mention here, and wishes to thank his advisor, Phil Rogaway, for not getting angry when time is wasted not doing real work.

The author would also like to thank his mother for teaching him to always put things back.

References

[1] John Black. *One-Time Pad without Irreducible Polynomials*. In Preparation. 1999.

[2] Lars Knudsen and Fauzan Mirza. *Deletion Cryptanalysis*. *Journal of Craptology* **1** (1999).

[3] Claude Shannon I think?! Not sure, but probably someone else thought of it first anyway.