Comments on the Rediscovery of Time Memory Data Tradeoffs[⋆]

Christophe De Cannière[⋆⋆] and Joseph Lano[⋆⋆⋆] and Bart Preneel

Katholieke Universiteit Leuven
Dept. Elect. Eng.-ESAT/SCD-COSIC,
Kasteelpark Arenberg 10, 3001 Heverlee, Belgium
{christophe.decanniere,joseph.lano,bart.preneel}@esat.kuleuven.be

Abstract. In this note we discuss the new Time Memory Data Tradeoffs for stream ciphers discussed by Hong and Sarkar in [3]. We investigate into more detail what threat these attacks pose for stream ciphers and relate this to the ECRYPT Call for Stream Cipher Primitives.

1 Introduction

In [3], Hong and Sarkar make the following important observation for stream ciphers: it has always been assumed that, in order to be resistant to Time Memory Data Tradeoff (TMD) attacks, a stream cipher has to have a state that is at least twice as large as the secret key length. They show that the TMD attack can easily circumvent this large state by working with the key directly. So it seems that the adoption of a state twice as large as the key is useless, unless we also use an IV which is as large as the key so as to add entropy to the scheme.

In this note we first show the implications of the attack, and make this explicit for the two cases in the ECRYPT call, namely a 128 bit key with a 64 bit IV and a 80 bit key with a 32 bit IV . We then discuss to what extent this can be a problem and draw an analogy with the birthday attack. We then propose a possible change of the ECRYPT call for papers.

2 Notations of the TMD attack

We have a stream cipher with a key of k bits and an IV of v bits. Now suppose we want to mount a TMD attack. The idea is that we observe a number of frames

[⋆] This work was supported in part by the Concerted Research Action (GOA) Mefisto 2000/06 of the Flemish Government and in part by the European Commission through the IST Programme under Contract IST2002507932 ECRYPT. The in formation in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

[⋆⋆] F.W.O. Research Assistant, sponsored by the Fund for Scientific Research - Flanders (Belgium)

[⋆⋆⋆] Research financed by a Ph.D. grant of the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen)

2^d, use precomputation time 2^p, and then mount an online attack using 2^t time and 2^m memory which permits us to recover the secret key of one frame. Note that if we recover one frame key, this can be used to recover up to 2^v frames that all may have used this secret key.

The TMD attack now has to satisfy the following constraints:

$$\begin{cases} p = k + v - d \\ t \geq 2d \\ t + m = k + v\,. \end{cases} \tag{1}$$

We will now study this tradeoff into more detail in the following section.

3 Two important bounds on the attack

A question that arises naturally is how much precomputation you can allow to have a realistic attack. An attack with precomputation time equal than or smaller than exhaustive search is a concern. But an attack with precomputation time larger than exhaustive search may also be a problem, certainly for schemes which are only designed to offer medium-term security. We will discuss this into more detail when looking into the ECRYPT cases.

3.1 A first case: $p \leq k + v$

A first question we ask ourselves is when we can mount a TMD attack in which p, t, d and m complexities are all smaller than exhaustive key search. The TMD formulas (1) give us an easy answer: Such an attack can be mounted if the IV size is smaller than half the key size.

3.2 A second case: no restriction imposed on p

A second question is when we can mount a TMD attack in which we pose no restrictions on p, but still want t, d and m complexities all smaller than exhaustive key search. Again, we can easily obtain the answer from the TMD formulas (1): Such an attack can be mounted if the IV size is smaller than the key size.

Note that increasing the precomputation time indefinitely does not keep improving the complexity of the best TMD attack (we take here as a rough measure for the complexity of the online phase $t + m + d$). It can be calculated that one gets the optimum tradeoff as soon as $p = 3/4 \cdot (k + v)$. We then have that $t = m = 1/2 \cdot (k + v)$ and $d = 1/4 \cdot (k + v)$.

4 Application of these bounds on the ECRYPT CfP

4.1 Profile 1

In Profile 1, ECRYPT looks for stream ciphers with a 128 bit key and an IV of (at least) 64 bits. We can see a graph of the TMD tradeoff in Fig. 1.

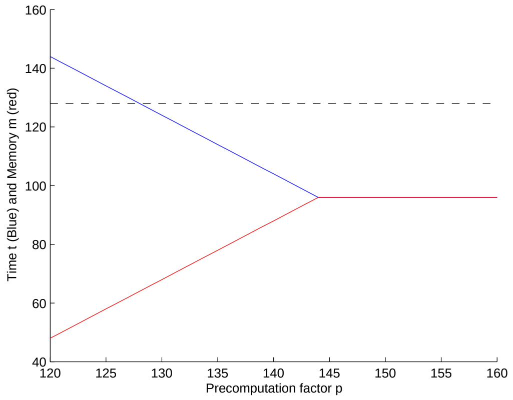

Fig. 1. TMD for Profile 1 stream cipher

In this figure, we show the points that minimize the maximum of t, m and d given the constraints of the TMD attack in (1). We see that the first case does not apply as the key is exactly twice the IV size, but we do have a TMD attack of the second type. The bifurcation point occurs for $p = 3/4 \cdot (128 + 64) = 144$, then $t = m = 1/2 \cdot (128 + 64) = 96$ and $d = 1/4 \cdot (128 + 64) = 48$.

4.2 Profile 2

In Profile 2, ECRYPT looks for stream ciphers with a 80 bit key and an IV of (at least) 32 bits. We can see a graph of the TMD tradeoff in Fig. 2.

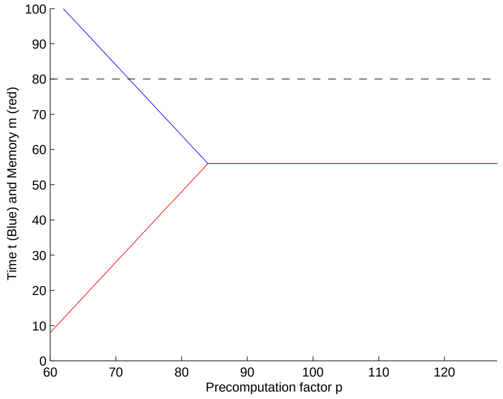

Fig. 2. TMD for Profile 2 stream cipher

In this figure, we show the points that minimize the maximum of t, m and d given the constraints of the TMD attack in (1). We see that the first case does apply as the key is more than twice the IV size. For instance, a point on the graph is $p = 79$, $t = 66$, $m = 48$ and $d = 39$. We also have a TMD attack of the second type. The bifurcation point occurs for $p = 3/4 \cdot (80 + 32) = 84$, then $t = m = 1/2 \cdot (80 + 32) = 56$ and $d = 1/4 \cdot (80 + 32) = 28$.

5 Evaluation of these attacks

To comment on these attacks, we first address a similar discussion, namely the birthday attack (which, for stream ciphers, amounts to the Babbage-Golic tradeoff [1, 2]): Suppose we generate keystream for 2^m key/IV pairs and store them in a table. We then observe 2^d different keystreams we are trying to attack. By the birthday paradox, we will be able to break one of these keystreams when $m = d = (k + v)/2$. *As long as the IV size is smaller than the key size, these complexities are lower than exhaustive search.*

Note that this also is a generic attack on all stream ciphers. Whether it is a real threat is a matter of discussion. The same also applies to the TMD attacks described here, as these attacks can also break only one frame out of the d observed frames.

Note also that this birthday attack also applies to block ciphers in ECB mode (and some other modes), and this in the following way. For a block cipher with key size k; you compute the output (for a fixed input) for $2^p = 2^m = 2^i$ random keys, and can then mount an attack using $2^t = 2^d(k - i)$. As for now, this is not regarded as a weakness for block cipher modes, but in analogy with stream ciphers this may become a topic of further discussion.

We think these kind of attacks can indeed be a problem. First, the complexities which can be found for Profile 2 with the 32 bit IV can indeed be seen as a threat. Second, because of the resynchronization mechanism, breaking one frame often gives us the key for breaking many frames. And third, the paper has shown us that it makes no sense to increase the state space without increasing the IV size.

In order to avoid this problem altogether, we think the best policy will be to take an IV which is as large as the key. As the state is already at least twice the key size, the designers should be able to adapt their design without too much difficulty to this new requirement. Certainly for Profile 2 one may want to do this, as it may be economically profitable for an attacker to do a precomputation that takes longer than exhaustive search. In the case of Profile 1 we think this threat is less obvious (we interpret long-term security as being largely unattainable, both for exhaustive search as for precomputation), but it would be interesting to hear within ECRYPT what are the opinions on this attack.

The only drawback for a longer IV is that the resynchronization mechanism may be slightly slower. Also there will have to be a good method to choose the first IV in a way that is not predictable to the attacker. (from then onwards a counter can be used to generate the other IVs, if the resync mechanism is sound).

References

1. Steve Babbage, *Improved exhaustive search attacks on stream ciphers*, European Convention on Security and Detection, IEE Conference publication No. 408, pp. 161–166, IEE, 1995.
2. Jovan Golic, *Cryptanalysis of alleged A5 stream cipher*, in Advances in Cryptology – EUROCRYPT 1997 (W. Fumy, ed.), LNCS 1233, pp. 239–255, Springer-Verlag, 1997.
3. Jin Hong and Palash Sarkar, *Rediscovery of the Time Memory Tradeoff*, Cryptology ePrint Archive, Report 2005/090, 2005.