MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Onewayness is closed under iterative hashing). *Let $h : \mathcal{S} \times \mathcal{S} \to \mathcal{S}$ be (t, ε)-oneway function. Show that function families defined by the construction*

$$\begin{aligned} g_2(m_1, m_2) &= h(m_1, m_2) \ , \\ g_3(m_1, m_2, m_3) &= h(g_2(m_1, m_2), m_3) \ , \\ &\ldots \end{aligned}$$

are also one-way functions. Explain how is this result can be generalised to Merkle trees.

Solution.

Simplified problem. Let us prove the onewayness of g_2. Let there be a collision, i.e., ... Then ...

General solution. The analysis done above is suitable for any i. Indeed, let g_{i-1} be ....

Qualitative analysis. Note that the success bound grows ...