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

Exercise (Naor commitments with extended message space). *The main drawback of the Naor commitment scheme is message expansion – to commit one bit one must send n bits. One possibility is to increase the size of the message space. Let the message space $\mathcal{M}$ be a subset of a finite field $(\mathbb{F}_{2^n}; +, \times)$ such that we can treat all n-bit strings as elements of $\mathbb{F}_{2^n}$. Then we can define modified commitment scheme:*

Gen	$\mathsf{Com}_{\mathsf{pk}}(x)$	$\mathsf{Open}_{\mathsf{pk}}(c,d)$
$\mathsf{pk} \xleftarrow{u} \mathbb{F}^*_{2^n}$	$d \leftarrow \{0,1\}^k$	$y \leftarrow c \oplus f(d)$
return pk	$c \leftarrow f(d) + x \times \mathsf{pk}$	if $y \notin \mathsf{pk} \times \mathcal{M}$ then ***return*** $\perp$
	return (c,d)	else ***return*** $y \times \mathsf{pk}^{-1}$

Establish the corresponding security guarantees under the assumption that $f : \{0,1\}^k \to \{0,1\}^n$ is a (t_1, ε_1)-pseudorandom generator. How big must be the message space $\mathcal{M} \subseteq \mathbb{F}_{2^n}$ to achieve reasonable security guarantees against double openings?

Solution.

Binding. The outcome c, d_1, d_2 of an adversary $\mathcal{A}$ can be double opening only if pk is a solution to equation .... As this equation can have at most ... solutions the number of public keys that can lead to a double opening is bounded by .... Consequently, ...

Hidding. Recall that commitment scheme is (t,ε)-hiding if any t-time adversary ... Recall that a function f is a (t,ε)-pseudorandom generator if ...

Qualitative analysis of the binding bound.... as a result the size of the message space $\mathcal{M}$ is bounded by ...