From: Peralta, Rene (Fed)
To: Calik, Cagdas (IntlAssoc)
Cc: Sonmez Turan, Meltem (Fed)
Subject: Re: MC of the Counting function (8,4) is 6.
Date: Friday, September 16, 2016 8:36:37 AM

Well, I don't think that "proof" makes any sense now.
I am looking at the problem again.

Regards, Rene.

From: Peralta, Rene (Fed)
Sent: Thursday, September 15, 2016 6:35 PM
To: Calik, Cagdas (IntlAssoc)
Cc: Sonmez Turan, Meltem (Assoc); Peralta, Rene (Fed)
Subject: Re: MC of the Counting function (8,4) is 6.
Great. I have a PQC meeting tomorrow, but maybe I will skip it. Let us play it by ear.

I am attaching what I think is the proof we needed (I think what you wanted is that the multiplicative complexity of

uv f

(where u,v are variables and f is a function of variables other than u,v)

is 1 + mult_comp(v f)

That is a corollary of the claim in the attached.

Regards, Rene.

****
Dr. Rene Peralta
Computer Security Division
NIST
(301) 975-8702

100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930
****

From: Calik, Cagdas (IntlAssoc)
Sent: Thursday, September 15, 2016 4:48 PM
To: Peralta, Rene (Fed)
Cc: Sonmez Turan, Meltem (Assoc)
Subject: MC of the Counting function (8,4) is 6.

Hi Rene,

By using the same approach (reducing the number of variables after affine transformations) we were able to find a 6 multiplication implementation of the counting function E(8,4). In your “Tight Bounds…” paper with Joan, the MC of this function was left as an open question, it could be either 6 or 7.

We hope to give you the details of the implementation tomorrow morning.

Cagdas & Meltem