Subject: Re: [COST:] IC1104, WG3 report
From: "Blackburn, S" <S.Blackburn@rhul.ac.uk>
Date: 06/10/14 10:34
To: Marcus Greferath <marcus.greferath@ucd.ie>

Dear Marcus,

Apologies for the silence: the start of term has caused some delays in my emailing.

I hope Palmela went well. It's a great shame I wasn't able to make it. The next MC meeting will be in ALCOMA, I assume? Though I also see that there is a meeting in Barcelona that Angeles and Camilla are organising (which I'll do my best to attend: will you be there?).

Here is a very short report (much shorter than Angeles', but I believe there is less activity in WG3 than WG2). If there is anything I have missed (in particular any visits and papers you know that I am unaware of) then please tell me.

One highlight of the recent activity in the WG is the proposal by Joachim Rosenthal for a McEliece-style cryptosystem based on orbit subspace codes. Such cryptosystems are very topical, due to the ongoing search for new primitives that might remain secure if quantum computers become practical ('post-quantum cryptography'). It is exciting that techniques from network coding are contributing to these developments.

COST participants Arsenia Chorti, Camilla Hollanti and David Karpuk have collaborated with Medhi Molu and Alister Burr to design strong physical layer wireless network security solutions to maintain data confidentiality: the paper Strong secrecy in wireless network coding systems with M-QAM modulators was presented at the 2014 Symposium on Privacy and Security in Commutations this summer.

Camilla Hollanti has also written the paper "Secrecy capacity of heterogeneous distributed storage systems", coauthored with COST participant Toni Ernvall, and with Salim El Rouayheb and Vincent Poor. This paper has appeared in Proceedings of the International Symposium on Communications, Control and Signal Processing (ISCCSP 2014).

Other WG members continue discussions on the interrelationships of ideas from network coding and cryptography. For example COST participants Simon Blackburn and Tuvi Etzion, with Maura Paterson, have discussed how techniques for Private Information Retrieval can be applied in settings where network coding techniques are recommended.

All the best,

Simon

Simon R. Blackburn
Professor of Pure Mathematics
Department of Mathematics
Royal Holloway University of London
Egham, Surrey TW20 0EX, United Kingdom
Tel: (+44) (0)1784 443422

Fax: (+44) (0)1784 430766
E-mail: S.Blackburn@rhul.ac.uk
Web: http://www.ma.rhul.ac.uk/sblackburn

From: Marcus Greferath <marcus.greferath@ucd.ie>
Date: Thursday, 2 October 2014 14:31
To: Simon Blackburn <s.blackburn@rhul.ac.uk>
Subject: [COST:] IC1104, WG3 report

dear simon,

i cannot find the report that you might have sent to me regarding work in WG3.
this is needed for the minutes of the recent MC meeting.

would you mind resending it to me? attached you can see a file that angeles sent
to me, and which i feel is very nice.

greetings, and thanks in advance.

marcus.

On 08/08/14 13:30, Blackburn, S wrote:

> Dear All,
>
> For WG3, I suggest starting with a 20 minute talk by Farhad Ghaboussi (Konstantz) "A construction of elliptic curves with rational solutions for cryptography", followed by a 20 minute talk by Joachim Rosenthal (Zurich) on a McEliece cryptosystem based on orbit subspace codes. The remaining time can be discussion.
>
> Marcus: since I will not be at the meeting, we need someone to lead the discussion. Joachim and Tuvi have very kindly volunteered to do this, unless you have someone else you think would be more appropriate. What do you think?
>
> I should say that I am now away from my email for two weeks from today: many apologies for any inconvenience caused.
>
> All the best,
>
> Simon
>
> ---
> Simon R. Blackburn
> Professor of Pure Mathematics
> Department of Mathematics
> Royal Holloway University of London
> Egham, Surrey TW20 0EX, United Kingdom
> Tel: (+44) (0)1784 443422

> Fax: (+44) (0)1784 430766
> E-mail: S.Blackburn@rhul.ac.uk
> Web: http://www.ma.rhul.ac.uk/sblackburn

--
Sent from my Commodore 64

Dr. Marcus Greferath
School of Mathematical Sciences
University College Dublin
Belfield, Dublin 4
Ireland

Phone: ++353-1-716-2588 (office)
++353-1-905-3085 (home)
++353-85-153-0951 (mobile)
Fax: ++353-1-716-1172
email: marcus.greferath@ucd.ie