

File 20100818.0751: Notes for WAR: pressure increasing to get preliminary results ready for confirmation.

I spent a lot of time getting an old laptop ready to take on this trip, but after I had gotten the distribution installed, got X working, and wireless working, the machine began overheating and finally died. At least it did it here and not in France. I will take my regular laptop instead (three times the size of the little one, but it works).

Andrea started a new job this week full-time as librarian for the Denver schools. For a week I have been taking care of Miranda, until the new school begins next week.

I gave a talk Friday to an audience of eighty-nine information assurance engineers at Lockheed on the subject of Gentry's fully homomorphic encryption. Extrapolating from the development of RSA, I predicted that FHE will become commercially viable in 2014 after efficient-enough implementations are developed and the security of the algorithm has been vetted by cryptographers. The most immediate application is to cloud computing, where FHE permits cloud users to upload large amounts of sensitive information to the cloud without risk of disclosure either to the cloud provider or third parties. A cloud provider could securely perform CFD, molecular modelling, seismic data analysis, or handling of credit card data and PII or personal data on extremely large data sets without risk of misplacing the information. Instead of cloud computing being relegated to non-sensitive information or being used only for remote storage of encrypted data, it could finally be used for sensitive information.

One question that came up in discussion afterwards was integrity of information under FHE. I suggested that remote attestation would dovetail with FHE to guarantee trustability at a lower level, with distributed toolkits like Hadoop serving to complete the availability triad.

I filed the security paperwork for foreign travel with Lockheed, the Navy, and NSA.

Going through MATLAB tutorial.

Itinerary:

- 20th August: United Airlines flight 908 from Denver, Colorado to Chicago; United flight 940 from Chicago to Frankfurt, Germany; 21st August: Lufthansa 9202 from Frankfurt to Nice, France.
- Hotel Novotel Nice Aeroport Cap 3000, 40 avenue du Verdun, 06700 Saint Laurent du Var
- 28th August: Lufthansa 9055 from Nice to Frankfurt; Lufthansa 8811 from Frankfurt to London Heathrow; United 939 from LHR to DEN.

References