Cryptography for Computer Scientists 2018/19 Dec 5, 2018

Exercises 10

Stefan Dziembowski MIM UW

Exercise 1: Physically secure banknotes

Some physical banknotes (e.g. the US dollars, see Fig. 1) have color fibers distributed evenly throughout the paper. Invent a method for making banknotes that are hard to forge, assuming the following physical property of the banknotes:

> *it is* easy *to produce a banknote with a random distribution of fibers, but it is* hard *to produce a banknote with a* given *distribution of fibers.*

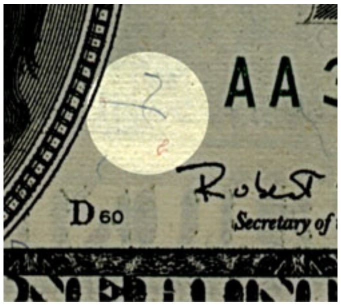

Figure 1: Fibers in a US dollar banknote

You can use digital signature schemes and assume that in order to test authenticity of a banknote one can scan electronically the pattern of the fibers on a banknote. Try to make your solution resilient against small errors in scanning the fiber patterns.

Exercise 2: Blind signatures

Blind signature schemes have a property that the signer does not learn the signed message (as a physical analogue of this think of signing messages in closed envelops). Design a bind signature scheme from the RSA cryptosystem.