

Homework 7

**Problem 7.1, 15 points.** Assume a public-key encryption scheme for single-bit messages (i.e. the message space is  $\{0,1\}$ ). Show that, given a public key  $pk$  and a ciphertext  $c$  computed by encrypting a random message  $m$  under  $pk$ , it is possible for an unbounded adversary to determine  $m$  with probability 1. (That shows that perfectly-secret public-key encryption is impossible.)

**Problem 7.2, 30 points.** We define a digital signature scheme  $\mathcal{DS}_{k,l} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$  which has two parameters: an integer  $k$  (the RSA modulus size) and an integer  $l$ . The message space for the scheme is  $\{0,1\}^l$ . For any  $l$ -bit message  $M$  let  $M_j$  denote its  $j$ -th bit, for  $j = 1, \dots, l$ . Then the key generation, signing and verifying algorithms are as follows:

<p>Algorithm <math>\mathcal{K}</math>  <math>(N, e), (N, d) \xleftarrow{\\$} \mathcal{K}_{rsa}</math>          For <math>b = 0, 1</math> do              For <math>j = 1, \dots, l</math> do                  <math>Y[b, j] \xleftarrow{\\$} \mathbb{Z}_N^*</math>              EndFor          EndFor          Return <math>(N, e, Y), (N, d, Y)</math></p>	<p>Algorithm <math>\mathcal{S}_{(N,d,Y)}(M)</math>          For <math>j = 1, \dots, l</math> do              <math>X[j] \leftarrow (Y[M_j, j])^d \bmod N</math>          EndFor          Return <math>X</math></p>	<p>Algorithm <math>\mathcal{V}_{(N,e,Y)}(M, X)</math>          flag <math>\leftarrow 1</math>          For <math>j = 1, \dots, l</math> do              If <math>(X[j])^e \bmod N \neq Y[M_j, j]</math>                  Then flag <math>\leftarrow 0</math>              EndIf          EndFor          Return flag</p>
--	--	--

Here  $\mathcal{K}_{rsa}$  is the standard RSA key generation algorithm. The public scheme of our scheme consists of the RSA modulus  $N$ , the RSA public exponent  $e$ , and a 2 by  $l$  array  $Y$  each of whose entries is a random point in  $\mathbb{Z}_N^*$ . The secret key is the RSA modulus  $N$ , the RSA secret exponent  $d$ , and the same array  $Y$ . The size of  $N$  is  $k$  bits. The signature of  $M$  is a one-dimensional array  $X$  of size  $l$  consisting of pre-images under  $RSA_{N,e}$  of certain points in the two-dimensional array  $Y$ , one per column of  $Y$ , the choice of which row being made according to the corresponding bit in the message.

Here is a picture for  $l = 4$ . On the left it pictures the array  $Y$ . On the right it pictures how you can think of the signature  $X$  of message  $M = 1001$ , namely as the inverses of certain points in the array on the left.

Y[0,1]	Y[0,2]	Y[0,3]	Y[0,4]
Y[1,1]	Y[1,2]	Y[1,3]	Y[1,4]

	X[2]	X[3]	
X[1]			X[4]

(a) [10 points] Show that this scheme is not UF-CMA secure. Your adversary has to have uf-cma - advantage 1 and make at most two queries to the signing oracle.

(b) [20 points] Show that this scheme is uf-cma secure as long as the adversary makes at most one query to its signing oracle, and RSA is one-way. More precisely, show that for any adversary  $F$  who attacks uf-cma security of  $\mathcal{DS}$  and makes at most one query to the signing oracle there exists an adversary  $I$  who attacks one-wayness of RSA such that

$$\text{Adv}_{\mathcal{DS}_{k,l}}^{\text{uf-cma}}(F) \leq 2l \cdot \text{Adv}_{\mathcal{K}_{rsa}}^{\text{ow-kea}}(I)$$

and you will have to specify  $I$ 's resources as a function of  $k$ ,  $l$  and the resources of  $F$ .

**Problem 7.3, 20 points.** In class we studied the ElGamal signature scheme (see the slides). In the original version of the ElGamal signature scheme the message space was  $Z_q$ , there was no hash function, and instead of  $H(M||Y)$ , the message  $M$  itself was used. Show that the original version is not uf-cma secure.