Solution Sheet #7

Advanced Cryptography 2022

Solution 1 DSS Security Hypothesis

1. We compute the discrete logarithm of the public key with respect to the base g and obtain the secret key which trivially allows to sign any message.

2. We can easily forge a triplet (h, r, s) as follows. Pick random elements α and β in $\mathbf{Z}_q^*$. Then, compute

$$r = (g^\alpha y^\beta \bmod p) \bmod q, \quad s = \frac{r}{\beta} \bmod q, \quad \text{and} \quad h = s\alpha \bmod q.$$

   From this, we see that a message m such that $H(m) = h$ passes the DSS verification with the signature (r, s), since

$$r = \left(g^{\frac{h}{s} \bmod q} y^{\frac{r}{s} \bmod q} \bmod p\right) \bmod q$$

   holds. If we invert H on h, we obtain a valid (m, r, s) triplet.

3. For two different messages m_1 and m_2, we create a collision $H(m_1) = H(m_2)$, then we ask for the signature (r, s) of m_1. The (m_2, r, s) triplet is a valid forged one.

4. If we can guess k we can compute $x = \frac{sk - H(m)}{r} \bmod q$. By brute force, guessing k requires within $\Omega(q)$ trials.

Solution 2 Instances of the ElGamal

1. $q = p - 1$. The IND-CPA security is equivalent to the hardness of the decisional Diffie-Hellman problem with generator g. However, the order of g is even so the least significant bit of the discrete logarithm of any $z \in \mathbf{Z}_p$ is easy to compute from the Legendre symbol $\left(\frac{z}{p}\right)$. Hence, we can easily distinguish (g, g^x, g^r, g^{xr}) from (g, g^x, g^r, g^s) by checking that the least significant bit of xr is the product of the least significant bits of x and r.

   Indeed, an adversary can select two messages m_0 and m_1 such that the least significant bit of $\log e(m_b)$ is b. (Given a random m, $\log e(m)$ is a random bit with distribution close to uniform, so we can easily find m_0 and m_1.) Then, given the encryption (u, v) of m_b, he can compute $b = \log(vu^{-x}) = \log v - (\log y) \log u$. So, the ElGamal cryptosystem is not IND-CPA secure.

2. In this case, the decisional Diffie-Hellman problem is assumed to be hard. We know that the IND-CPA security in this case is equivalent to the decisional Diffie-Hellman problem. So, the ElGamal cryptosystem is IND-CPA secure.

   It is pretty hard to propose an efficient embedding because e must be invertible in practice.

3. Yes. This is a particular case of the previous question.

   We know that the group of quadratic residues includes exactly $\frac{p-1}{2} = q$ elements. We know that $\mathcal{G}$ has q elements. Furthermore, $g^{\frac{p-1}{2}} = g^q = 1$ so g is a quadratic residue. So, all elements of $\mathcal{G}$ are quadratic residues. Therefore, all quadratic residues are in $\mathcal{G}$.

   We have $(-1)^{\frac{p-1}{2}} = (-1)^q = -1$ so the Legendre symbol is -1.

   Either x or $-x$ is a quadratic residue but not both since -1 is not a quadratic residue. So, either x or $-x$ is in $\mathcal{G}$.

   Let $e_0(m) - 1$ be the integer with binary expansion m. We have $0 < e_0(m) \leq q$. Let now $e(m) = e_0(m)$ if $\left(\frac{e_0(m)}{p}\right) = +1$ and $e(m) = -e_0(m)$ otherwise. We have $e(m) \in \mathcal{G}$. Since we cannot have $e(m) = e(m')$ whenever $m \neq m'$, this is a practical embedding function. Its inverse is also easy to compute.

Solution 3 PIF implies PAF

Consider an adversary $\mathcal{A}$ who is polynomially bounded. We want to show that $p = \Pr[\mathsf{PAF}(\mathcal{A}, 1^\lambda) = 1]$ is negligible.

For this, we define the adversary $\mathcal{A}'$ as follows: we let $\rho' = r' \| \rho \| b''$ and $\mathcal{A}'(\rho')$ picks a random x using r'. Then, $\mathcal{A}'(y; \rho')$ runs $\mathcal{A}(y; \rho) = x''$. If $x = x''$, it answers 1. Otherwise, it answers by b''.

When running the game $\mathsf{PIF}(\mathcal{A}', 1^\lambda)$, in the $b = 0$ case, we have $x = x''$ with probability p and $\mathcal{A}'$ answers 1. We have $x \neq x''$ with probability $1 - p$ and $\mathcal{A}'$ answers 1 with probability $\frac{1}{2}$. So, $\mathcal{A}'$ answers 1 with probability $p + \frac{1-p}{2}$. So,

$$\Pr[\mathsf{PIF}(\mathcal{A}', 1^\lambda) = 1 | b = 0] = p + \frac{1-p}{2}$$

When $b = 1$, $\mathcal{A}(y; \rho)$ has no information about x, so x is independent from x'' and we have $\Pr[x = x''] = 2^{-\lambda}$. Thus,

$$\Pr[\mathsf{PIF}(\mathcal{A}', 1^\lambda) = 1 | b = 1] = 2^{-\lambda} + \frac{1 - 2^{-\lambda}}{2}$$

Finally, we have

$$\begin{aligned} \Pr[\mathsf{PIF}(\mathcal{A}', 1^\lambda) = 1] - \frac{1}{2} &= \frac{1}{2}\left(p + \frac{1-p}{2} + 2^{-\lambda} + \frac{1 - 2^{-\lambda}}{2}\right) - \frac{1}{2} \\ &= \frac{p}{4} + \frac{2^{-\lambda}}{4} \end{aligned}$$

Since F_k is PIF-secure, we know that $\Pr[\mathsf{PIF}(\mathcal{A}', 1^\lambda) = 1] - \frac{1}{2}$ must be negligible. Thus, $\frac{p}{4} + \frac{2^{-\lambda}}{4}$ is negligible. Since $\frac{2^{-\lambda}}{4}$ is negligible, we obtain that $\frac{p}{4}$ is negligible. So, p is negligible.