VE475 Homework 7

Yiwen Yang

Ex. 0 - Merkle-Damgård Construction

1. (a) For any y, we can derive x by checking from the tail: if last bit is 0, then $x_i = 0$; else last two bits must be 01, then $x_i = 1$. The result of x is unique, so there is no different x' that can produce the same y, then s is injective.

   (b) If z is empty, then from (a) we know that no $s(x) = s(x')$. If z is not empty, since all $s(x')$ starts with 11, and we cannot find two adjacent 1 of $s(x)$ which consists of only 0 and 01 (except at the beginning), so $s(x)$ cannot be $z \parallel s(x')$.

2. (a) is important because if s is not injective, then we can found $x \neq x'$ such that $y = y'$, which contributes a collision to h. (b) is important because if the condition is true, then we can pad z in front of $s(x')$ to find another $s(x)$; When z' is empty, this means $g(z' \parallel s(x)) = g(z \parallel s(x'))$ and this is a collision.

3. Assume there is a collision on h, $x \neq x'$ such that $h(x) = h(x')$, we will prove that a collision on the compression function g can be efficiently found.

   First, if x and x' has the same block numbers, i.e. $k = k'$, then $y_k = y_{k'}$.

   $$g(z_{k-1} \parallel y_k) = g(z_{k'-1} \parallel y_{k'})$$

   If $z_{k-1} \neq z_{k'-1}$, then collision if found. Otherwise repeat the process, then either we find a collision or at last $z_1 = z_{1'} \dots z_k = z_{k'}$, which contradicts.

   Next, if x' is longer than x, i.e. $k' > k$, repeat the same process as above and either find a collision or at last but not least

   $$g(z_1 \parallel y_2) = g(z_{k'-k} \parallel y_{k'-k+1})$$

   Since $y_2 = 1$, if $y_{k'-k+1} = 0$ then collision if found. Else $y_{k'-k+1} = 1$, $y_{k'-k} = 0$ because there is no continuous two 1 in y except at the beginning. Then

   $$z_1 = z_{k'-k}$$

   $$g(0^m \parallel y_1) = g(z_{k'-k-1} \parallel y_{k'-k})$$

   Then collision is found since $y_1 = 1$ while $y_{k'-k} = 0$.

   Above all cases, h should be collision resistant if h is collision resistant.

Ex. 1 - Cramer-Shoup Cryptosystem

1. - **Key Generation**

     Given a cyclic group G of order q, find two random different generators g_1 and g_2. First, choose (x_1, x_2, y_1, y_2, z) from $\{0, \dots, q-1\}$ randomly. Then computes $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, $h = g_1^z$. Finally, $(G, q, g_1, g_2, c, d, h)$ are public keys, and (x_1, x_2, y_1, y_2, z) are private keys.

   - **Encryption**

     First choose a random k from $\{0, \dots, q-1\}$. Then computes $u_1 = g_1^k$, $u_2 = g_2^k$, $e = h^k m$, $\alpha = H(u_1, u_2, e)$, $v = c^k d^{k\alpha}$, where $H()$ is a universal one-way hash function. The cipher text is given as (u_1, u_2, e, v).

   - **Decryption**

     First computes $\alpha = H(u_1, u_2, e)$ with the same hash function and verifies that $v = u_1^{x_1} u_2^{x_2} (u_1^{y_1} u_2^{y_2})^\alpha$. If fails, then reject the decryption. Otherwise, the plain text is given by $m = e/(u_1^z)$.

2. This cryptosystem is IND-CCA2 secure because there is a verification step that checks whether the hash function gives the correct result, otherwise the whole encryption is rejected. This can prevent the attacker trying to discover some patterns when feeding the oracle with some invalid or forged ciphertexts.

3. Cramer-Shoup and Elgamal are both public key encryption algorithms based on DLP, while Cramer-Shoup is based on the computational intractability of DDH and Elgamal is based on both CDH and DDH. Elgamal is not IDN-CCA safe, while Cramer-Shoup is.

Ex. 2 - Simple Questions

1. For any given x, we can easily find $x' = x + p - 1$ such that $h(x) \equiv \alpha^x \equiv \alpha^{x+p-1} \equiv \alpha^{x'} \equiv h(x') \bmod p$, so h is neither collision resistant nor second pre-image resistant.

2. The results are 0x5a827999, 0x6ed9eba1, 0x8f1bbcdc and 0xca62c1d6, which are equal to the four constants in K.

Ex. 3 - Birthday Paradox

1. (a)

   $$g(x) = \ln(1-x) + x + x^2$$

   $$\frac{d}{dx} g(x) = \frac{1}{x-1} + 1 + 2x = \frac{2(x-\frac{1}{4})^2 - \frac{1}{8}}{x-1}$$

   When $x \in [0, \frac{1}{2}]$, $\frac{d}{dx} g(x) > 0$, so $g(x)$ is monotonically increasing. Note that $g(0) = 0$, then $g(x) \geq 0 \Rightarrow -x - x^2 \leq \ln(1-x)$.

(b)

$$h(x) = \ln(1-x) + x$$

$$\frac{d}{dx}h(x) = \frac{1}{x-1} + 1 = \frac{x}{x-1}$$

When $x \in [0, \frac{1}{2}]$, $\frac{d}{dx}h(x) < 0$, so $h(x)$ is monotonically decreasing. Note that $h(0) = 0$, then $h(x) \leq 0 \Rightarrow \ln(1-x) \leq -x$.

From above, $-x - x^2 \leq \ln(1-x) \leq -x$.

2. Since $r \leq n/2$, then $r/n \leq 1/2$. From (1) we can get

$$-\frac{j}{n} - \frac{j^2}{n^2} \leq \ln(1-\frac{j}{n}) \leq -\frac{j}{n}$$

$$\sum_{j=1}^{r-1}(-\frac{j}{n} - \frac{j^2}{n^2}) \leq \sum_{j=1}^{r-1}\ln(1-\frac{j}{n}) \leq \sum_{j=1}^{r-1}-\frac{j}{n}$$

$$-\frac{(r-1)r}{2n} - \frac{(r-1)r(2r-1)}{6n^2} \leq \sum_{j=1}^{r-1}\ln(1-\frac{j}{n}) \leq -\frac{(r-1)r}{2n}$$

On the left hand side

$$\frac{(r-1)r(2r-1)}{6n^2} = \frac{r^3 - \frac{3}{2}r^2 + r}{3n^2} < \frac{r^3}{3n^2}$$

So

$$-\frac{(r-1)r}{2n} - \frac{r^3}{3n^2} \leq \sum_{j=1}^{r-1}\ln(1-\frac{j}{n}) \leq -\frac{(r-1)r}{2n}$$

3. Let $\lambda = r^2/2n$, and $\lambda \leq n/8 \Rightarrow r \leq n/2$, then

$$-\frac{(r-1)r}{2n} - \frac{r^3}{3n^2} = -\lambda + \sqrt{\frac{\lambda}{2n}} - \frac{(2\lambda)^{3/2}}{3n^{1/2}} = -\lambda + c_1/\sqrt{n}$$

$$-\frac{(r-1)r}{2n} = -\lambda + \sqrt{\frac{\lambda}{2n}} = -\lambda + c_2/\sqrt{n}$$

Then take the exponential of (2) gets

$$e^{-\lambda + c_1/\sqrt{n}} \leq \prod_{j=1}^{r-1}(1-\frac{j}{n}) \leq e^{-\lambda + c_2/\sqrt{n}}$$

4. If λ is a constant, then c_1 and c_2 from (3) are all constants, which means that when n is very large, $e^{c_1/\sqrt{n}}, e^{c_2/\sqrt{n}} \to 1$. So $\prod_{j=1}^{r-1}(1-\frac{j}{n}) \risingdotseq e^{-\lambda}$.

Ex. 4 - Birthday Attack

1. $$1 - \prod_{i=1}^{39} \frac{1000 - i}{1000} = 0.546$$

   There is 0.546 probability to observe two plates with the same 3-digit ending.

2. $$C_{40}^{1} \frac{1}{1000} (\frac{999}{1000})^{39} = 0.038$$

   There is 0.038 probability to find one plate with 123 ending.

3. The probability of having two same birthday in a global range is very high, but if we select a certain birthday, then the collision rate will be much smaller. Similarly, Alice first chooses a hash to sign on, then the hash collision rate will be much lower than that of arbitrary two hash which Eve provides.

Ex. 5 - Faster Multiple Modular Exponentiation

1. $\mathcal{O}((\log n)^2 \log a + (\log n)^2 \log b) = \mathcal{O}((\log n)^2 \log ab)$

2. If $\alpha\beta$ is given, then the following algorithm can be used.

Algorithm 1 Faster multiple modular exponentiation

```
Input: $\alpha$, $a$, $\beta$, $b$, $n$, $\alpha\beta$
Output: $\alpha^a \beta^b$ mod $n$
  $k \leftarrow$ Max(Bit size of $a$, Bit size of $b$)
  $power \leftarrow 1$
  for $i \leftarrow k - 1$ downto 0 do
      $power \leftarrow power \cdot power$ mod $n$
      if $a_i = 1$ and $b_i = 1$ then
          $power \leftarrow power \cdot \alpha\beta$ mod $n$
      else if $a_i = 1$ then
          $power \leftarrow power \cdot \alpha$ mod $n$
      else if $b_i = 1$ then
          $power \leftarrow power \cdot \beta$ mod $n$
      end if
  end for
  return $power$
```

3. l squaring and l multiplications are necessary.

4. See source code in folder **ex5**. The results show that when calculating random 15360-bit numbers, the normal method takes 1.403902s and faster method takes 0.952246s (32% faster).