دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

عنوان: تکلیف اول درس مهندسی فناوری اطلاعات

نام و نام خانوادگی: علیرضا ابره فروش

شماره دانشجویی: ۹۸۱۶۶۰۳

نیم سال تحصیلی: پاییز ۱۴۰۱

مدرّس: دکتر محمدحسین منشئی

۱

$m = (00110010)_2 = (50)_{10}$

$p = 23, q = 19$

$n = pq = 23 \times 19 = 437$

$z = (p-1)(q-1) = 22 \times 18 = 396$

$e = 97 \Rightarrow e < n,\ (e, z) = 1$

$d = 49 \Rightarrow ed \equiv 1 (mod\, z)$

$c = (m^e \equiv 1 (mod\, n)) \Rightarrow c = 335$

$m = (c^d \equiv 1 (mod\, n)) \Rightarrow m = 50$

$K^+ = e = 97$

$K^- = d = 49$

۲

Trudy می‌تواند به سیستم نفوذ کند و محتوای ارسال شده را تغییر دهد. به این صورت که M و $H(M) + S$ را از هم جدا می‌کند. سپس با محاسبه‌ی hash پیامِ M و حذف آن از $H(M) + S$ (به شکل $H(M) + S - H(M)$) به shared secret دست پیدا می‌کند. سپس پیام مورد نظر خود (M') را به همراه $H(M')$ و S برای فرد به شکل $(M', H(M') + S)$ ارسال می‌کند.

۳

ستون A که به نسبت سایر ستون‌ها ضرایب بزرگتری دارد فاقد regularization term است. پس مربوط به تابع هزینه‌ی اول است.
ستون B فاقد ضرایب صفر است. می‌دانیم که امکان صفر شدن ضرایب در lasso regression موجود است. پس مربوط به تابع دوم است.
ستون C دارای ضرایب صفر است. می‌دانیم که در ridge regression هرگز ضرایب صفر نمی‌شوند. پس مربوط به تابع سوم است.

۴

هزاران نفر قصد دارند پیام Alice را دریافت کنند و Alice آماده است که پیام را به هر متقاضی بفرستد. برای تضمین صحت پیام، Alice می‌تواند ابتدا hashِ پیام را با private key خود رمز کند و همراه پیام $((m, K_A^-(H(m))))$ به هر یک از متقاضیان بفرستد. چون Alice تنها کسی است که private key خود را دارد و پیامی که با private key رمز شده است تنها با public key نظیر همان private key قابل رمزگشایی است، در این صورت هر یک از دریافت‌کننده‌های پیام می‌توانند صحت این پیام را احراز کنند. به این صورت که هر یک از دریافت‌کننده‌ها $K_A^-(H(m))$ و m را از هم جدا می‌کند. سپس با استفاده از Alice public key $H(m)$ را به شکلِ $H(m) = K_A^+(K_A^-(H(m)))$ به دست می‌آورد. در نهایت با گرفتن hash از m جدا شده و بررسی برابریِ آن با $H(m)$ به

دست آمده در مرحله‌ی قبل صحت پیام احراز می‌شود. توجه شود که برای دستیابی به صحت می‌توانستیم به جای مکانیزم امضای دیجیتال از MAC استفاده کنیم. اما در این حالت Alice باید به ازای هر دریافت‌کننده $(m, H(m+s))$ را محاسبه کند که خود این کار با توجه به تعداد زیاد دریافت‌کننده‌های پیام می‌تواند overhead قابل توجهی داشته باشد و همچنین لازم بود که به ازای هر دریافت‌کننده یک shared secret داشته باشد که مدیریت آن‌ها می‌تواند ساده نباشد.
پس در این جا استفاده از digital-signature-based integrity scheme نسبت به MAC algorithm scheme بهتر است.

۵

$$p(\mu|X) \propto p(x_k|\mu).p(\mu)$$

$$p(\mu|X) = \left[\prod_{k=1}^{n} \frac{1}{\sqrt{2\pi\sigma'^2}} e^{-\frac{(x_k-\mu)^2}{2\sigma'^2}}\right] . \frac{1}{(2\pi)^{\frac{l}{2}}\sigma_\mu^2} e^{-\frac{\|\mu-\mu_0\|^2}{2\sigma_\mu^2}}$$

$$\ln(p(\mu|X)) = \sum_{k=1}^{n}\left[-\ln\left(\sqrt{2\pi\sigma'^2}\right) - \frac{(x_k-\mu)^2}{2\sigma'^2}\right] - \ln\left((2\pi)^{\frac{l}{2}}\sigma_\mu^2\right) - \frac{\|\mu-\mu_0\|^2}{2\sigma_\mu^2}$$

$$\frac{\partial}{\partial\mu}\ln(p(\mu|X)) = 0$$

$$\sum_{k=1}^{n}\frac{x_k-\mu}{\sigma'^2} = \frac{\|\mu-\mu_0\|}{2\sigma_\mu^2}$$

$$\mu = \frac{\frac{\sum_{k=1}^{n} x_k}{\sigma'^2} + \frac{\mu}{2\sigma_\mu^2}}{n + \frac{1}{2\sigma_\mu^2}}$$

۶

$\mathcal{L}(w)$: تابع هزینه
$\mathcal{L}_i(w)$: هزینه‌ی training example ِiام
w^t: وزن‌ها در گام tام

$$y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_9 \end{bmatrix}, X = \begin{bmatrix} (X_1)^2 & X_1 & 1 \\ (X_2)^2 & X_2 & 1 \\ \vdots & \vdots & \vdots \\ (X_9)^2 & X_9 & 1 \end{bmatrix}, w = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

$$\mathcal{L}_i(w^{(t)}) = \frac{1}{2}\left(y_i - X_i^T w^{(t)}\right)^2$$
$$\nabla\mathcal{L}_i(w^{(t)}) = -X_i\left(y_i - X_i^T w^{(t)}\right)$$

$$w^{(t+1)} = w^{(t)} - \alpha \nabla \mathcal{L}_i(w^{(t)})$$

$$w^{(0)} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$w^{(1)} = \begin{bmatrix} 0.00000000e+00 \\ 0.00000000e+00 \\ 0.00000000e+00 \end{bmatrix} - 0.1 \times \left(- \begin{bmatrix} 35.38^2 \\ 35.38 \\ 1 \end{bmatrix} \left(2955.53 - \begin{bmatrix} 35.38^2 & 35.38 & 1 \end{bmatrix} \begin{bmatrix} 0.00000000e+00 \\ 0.00000000e+00 \\ 0.00000000e+00 \end{bmatrix} \right) \right) =$$

$$\begin{bmatrix} 3.69956813e+05 \\ 1.04566651e+04 \\ 2.95553000e+02 \end{bmatrix}$$

$$w^{(2)} = \begin{bmatrix} 3.69956813e+05 \\ 1.04566651e+04 \\ 2.95553000e+02 \end{bmatrix} - 0.1 \times \left(- \begin{bmatrix} 15.32^2 \\ 15.32 \\ 1 \end{bmatrix} \left(560.30 - \begin{bmatrix} 15.32^2 & 15.32 & 1 \end{bmatrix} \begin{bmatrix} 3.69956813e+05 \\ 1.04566651e+04 \\ 2.95553000e+02 \end{bmatrix} \right) \right) =$$

$$\begin{bmatrix} -2.04129879e+09 \\ -1.33257738e+08 \\ -8.69867277e+06 \end{bmatrix}$$

$$w^{(3)} = \begin{bmatrix} -2.04129879e+09 \\ -1.33257738e+08 \\ -8.69867277e+06 \end{bmatrix} -0.1 \times \left(- \begin{bmatrix} 11.74^2 \\ 11.74 \\ 1 \end{bmatrix} \left(334.32 - \begin{bmatrix} 11.74^2 & 11.74 & 1 \end{bmatrix} \begin{bmatrix} -2.04129879e+09 \\ -1.33257738e+08 \\ -8.69867277e+06 \end{bmatrix} \right) \right) =$$

$$\begin{bmatrix} 3.89738346e+12 \\ 3.32015359e+11 \\ 2.82833471e+10 \end{bmatrix}$$

$$w^{(4)} = \begin{bmatrix} 3.89738346e+12 \\ 3.32015359e+11 \\ 2.82833471e+10 \end{bmatrix} - 0.1 \times \left(- \begin{bmatrix} 19.05^2 \\ 19.05 \\ 1 \end{bmatrix} \left(864.44 - \begin{bmatrix} 19.05^2 & 19.05 & 1 \end{bmatrix} \begin{bmatrix} 3.89738346e+12 \\ 3.32015359e+11 \\ 2.82833471e+10 \end{bmatrix} \right) \right) =$$

$$\begin{bmatrix} -5.15545092e+16 \\ -2.70614602e+15 \\ -1.42044054e+14 \end{bmatrix}$$

$$w^{(5)} = \begin{bmatrix} -5.15545092e+16 \\ -2.70614602e+15 \\ -1.42044054e+14 \end{bmatrix} -0.1 \times \left(- \begin{bmatrix} 26.85^2 \\ 26.85 \\ 1 \end{bmatrix} \left(1709.09 - \begin{bmatrix} 26.85^2 & 26.85 & 1 \end{bmatrix} \begin{bmatrix} -5.15545092e+16 \\ -2.70614602e+15 \\ -1.42044054e+14 \end{bmatrix} \right) \right) =$$

$$\begin{bmatrix} 2.68463555e+21 \\ 9.99856406e+19 \\ 3.72381873e+18 \end{bmatrix}$$

$$w^{(6)} = \begin{bmatrix} 2.68463555e+21 \\ 9.99856406e+19 \\ 3.72381873e+18 \end{bmatrix} - 0.1 \times \left(- \begin{bmatrix} 39.45^2 \\ 39.45 \\ 1 \end{bmatrix} \left(3670.48 - \begin{bmatrix} 39.45^2 & 39.45 & 1 \end{bmatrix} \begin{bmatrix} 2.68463555e+21 \\ 9.99856406e+19 \\ 3.72381873e+18 \end{bmatrix} \right) \right) =$$

$$\begin{bmatrix} -6.50851298e+26 \\ -1.64980998e+25 \\ -4.18201594e+23 \end{bmatrix}$$

$$w^{(7)} = \begin{bmatrix} -6.50851298e+26 \\ -1.64980998e+25 \\ -4.18201594e+23 \end{bmatrix} -0.1 \times \left(- \begin{bmatrix} 30.51^2 \\ 30.51 \\ 1 \end{bmatrix} \left(2202.93 - \begin{bmatrix} 30.51^2 & 30.51 & 1 \end{bmatrix} \begin{bmatrix} -6.50851298e+26 \\ -1.64980998e+25 \\ -4.18201594e+23 \end{bmatrix} \right) \right) =$$

$$\begin{bmatrix} 5.64425427e+31 \\ 1.84997346e+30 \\ 6.06351097e+28 \end{bmatrix}$$

$$w^{(8)} = \begin{bmatrix} 5.64425427e+31 \\ 1.84997346e+30 \\ 6.06351097e+28 \end{bmatrix} - 0.1 \times \left(- \begin{bmatrix} 3.98^2 \\ 3.98 \\ 1 \end{bmatrix} \left(13.08 - \begin{bmatrix} 30.51^2 & 30.51 & 1 \end{bmatrix} \begin{bmatrix} 5.64425427e+31 \\ 1.84997346e+30 \\ 6.06351097e+28 \end{bmatrix} \right) \right) =$$

$$\begin{bmatrix} -1.37156316e+33 \\ -3.56945428e+32 \\ -9.00889632e+31 \end{bmatrix}$$

$$w^{(9)} = \begin{bmatrix} -1.37156316e+33 \\ -3.56945428e+32 \\ -9.00889632e+31 \end{bmatrix} - 0.1 \times \left(- \begin{bmatrix} 0.29^2 \\ 0.29 \\ 1 \end{bmatrix} \left(2.28 - \begin{bmatrix} 0.29^2 & 0.29 & 1 \end{bmatrix} \begin{bmatrix} -1.37156316e+33 \\ -3.56945428e+32 \\ -9.00889632e+31 \end{bmatrix} \right) \right) =$$

$$\begin{bmatrix} -1.36896487e+33 \\ -3.47985832e+32 \\ -5.91938034e+31 \end{bmatrix}$$

در هر گام از بین training exampleها یکی را به صورت تصادفی انتخاب می‌کنیم. این کار را به تعداد training exampleها تکرار می‌کنیم تا کل داده‌ها توسط مدل دیده شوند.

منابع