Appendix

Proof of Theorem 1. Consider the characteristic of normal distribution that the sum of variable from normal distribution is also distributed as normal distribution (Eisenberg and Sullivan 2008), it is obvious that both of $\sum_{i\in\mathcal{R}_s^j}\mathbf{c}_{ij_s}$ and $\sum_{i\in\mathcal{R}_n^j}\mathbf{c}_{ij_n}$ are distributed as $N(0,1)$. Then based on Lemma 1, we know $\sum_{i\in\mathcal{R}_s^j}\mathbf{x}_j^i$ and $\sum_{i\in\mathcal{R}_n^j}\mathbf{y}_j^i$ are distributed as $Lap(\frac{2\Delta\sqrt{K}}{\epsilon_s})$ and $Lap(\frac{2\Delta\sqrt{K}}{\epsilon_n})$.

Let $\epsilon_s=(1+\beta)\epsilon$, $\epsilon_n=(\frac{1}{\beta}+1)\epsilon$, and $c=\sum_{i\in\mathcal{R}_s^j}\mathbf{c}_{ij_s}+\sum_{i\in\mathcal{R}_n^j}\mathbf{c}_{ij_n}$ which is obviously distributed as $N(0,1)$. Since every user keeps the same $\mathbf{h}_j$ when updates $\mathbf{v}_j$ in each iteration, the summation of these random noise vector for sensitive and non-sensitive ratings can be calculated as

$$\begin{aligned}\mathbf{p}_j=&\sum_{i\in\mathcal{R}_s^j}\mathbf{x}_j^i+\sum_{i\in\mathcal{R}_n^j}\mathbf{y}_j^i\\=&\frac{2\Delta\sqrt{2K\mathbf{h}_j}}{\epsilon_s}\sum_{i\in\mathcal{R}_s^j}\mathbf{c}_{ij_s}+\frac{2\Delta\sqrt{2K\mathbf{h}_j}}{\epsilon_n}\sum_{i\in\mathcal{R}_n^j}\mathbf{c}_{ij_n}\\=&2\Delta c\sqrt{2K\mathbf{h}_j}(\frac{1}{\epsilon_s}+\frac{1}{\epsilon_n})\\=&2\Delta c\sqrt{2K\mathbf{h}_j}\left(\frac{1}{(1+\beta)\epsilon}+\frac{1}{(\frac{1}{\beta}+1)\epsilon}\right)\\=&\frac{2\Delta\sqrt{K}}{\epsilon}\sqrt{2\mathbf{h}_j}c\end{aligned}$$

Then each element in $\mathbf{p}_j=\{p_{j1},p_{j2},...,p_{jl},...,p_{jK}\}$ is distributed as $Lap(\frac{2\Delta\sqrt{K}}{\epsilon})$ based on Lemma 1, which is equal to that we randomly picked each p_{jl} from the $Lap(\frac{2\Delta\sqrt{K}}{\epsilon})$ distribution, whose probability density function is $Pr(p_{jl})=\frac{\epsilon}{4\Delta\sqrt{K}}e^{-\frac{\epsilon|p_{jl}|}{2\Delta\sqrt{K}}}$.

Let D_1 and D_2 be two datasets only differ from one record $\mathbf{R}_{ab}$ and $\tilde{\mathbf{R}}_{ab}$, which can be sensitive or non-sensitive. From the different inputs D_1 and D_2, we obtain the same output, i.e., the same derived $\mathbf{V}$. Since the derived $\mathbf{V}$ are the optimized result after convergence, we then have $\frac{\partial\mathcal{J}(D_1)}{\partial\mathbf{v}_j}=\frac{\partial\mathcal{J}(D_2)}{\partial\mathbf{v}_j}=0$ as Eq.(8), which then can be formulated as,

$$2\sum_{i=1}^{n}\mathbf{I}_{ij}(\mathbf{u}_i^T\mathbf{v}_j-\mathbf{R}_{ij})\mathbf{u}_i+\mathbf{p}_j=2\sum_{i=1}^{n}\mathbf{I}_{ij}(\mathbf{u}_i^T\mathbf{v}_j-\tilde{\mathbf{R}}_{ij})\mathbf{u}_i+\tilde{\mathbf{p}}_j \tag{11}$$

As ratings in D_1 and D_2 only differs from $\mathbf{R}_{ab}$ and $\tilde{\mathbf{R}}_{ab}$, then we can get

$$\mathbf{p}_j-\tilde{\mathbf{p}}_j=2\mathbf{u}_i(\mathbf{R}_{ab}-\tilde{\mathbf{R}}_{ab}).$$

Considering $|\mathbf{R}_{ab}-\tilde{\mathbf{R}}_{ab}|\le\Delta$ and $||\mathbf{u}_i||\le 1$, it's obvious $||\mathbf{p}_j-\tilde{\mathbf{p}}_j||\le 2\Delta$.

We then formulate the probability that we get the same derived $\mathbf{V}$ with the different datasets D_1 and D_2 after convergence. For each vector $\mathbf{v}_j$ of $\mathbf{V}$, we have

$$\begin{aligned}\frac{Pr[\mathbf{v}_j|D_1]}{Pr[\mathbf{v}_j|D_2]}=&\frac{\prod_{l\in\{1,2,...,K\}}Pr(p_{jl})}{\prod_{l\in\{1,2,...,K\}}Pr(\tilde{p}_{jl})}\\=&e^{-\frac{\epsilon\sum_l|p_{jl}|}{2\Delta\sqrt{K}}}/e^{-\frac{\epsilon\sum_l|\tilde{p}_{jl}|}{2\Delta\sqrt{K}}}=e^{\frac{\epsilon\sum_l(|p_{jl}|-|\tilde{p}_{jl}|)}{2\Delta\sqrt{K}}}\\\le&e^{\frac{\epsilon\sqrt{K\sum_l(p_{jl}-\tilde{p}_{jl})^2}}{2\Delta\sqrt{K}}}=e^{\frac{\epsilon\sqrt{K}||\mathbf{p}_j-\tilde{\mathbf{p}}_j||}{2\Delta\sqrt{K}}}\le e^{\epsilon}\end{aligned}$$

So, we obtain the conclusion.

Proof of Theorem 2. With the characteristic of normal distribution and Lemma 1, we know $2\sum_{f\in\mathcal{F}_i}\mathbf{q}_i^f\sim Lap(\frac{2\sqrt{K}}{\epsilon})$.

Let D_1 and D_2 be two datasets only differ from one record $\mathbf{u}_i^f$ and $\tilde{\mathbf{u}}_i^f$. From the different inputs D_1 and D_2, we obtain the same output, i.e., the same derived $\mathbf{U}$. Since the derived $\mathbf{U}$ is the optimized results after convergence, then we know $\frac{\partial\mathcal{J}(D_1)}{\partial\mathbf{u}_i}=\frac{\partial\mathcal{J}(D_2)}{\partial\mathbf{u}_i}=0$ as Eq.(9), which can be formulated as,

$$\mathbf{q}_i^f+2\sum_{f\in\mathcal{F}_i}S_{if}(\mathbf{u}_i-\mathbf{u}_f)=\tilde{\mathbf{q}}_i^f+2\sum_{f\in\mathcal{F}_i}S_{if}(\mathbf{u}_i-\tilde{\mathbf{u}}_f) \tag{12}$$

As there's only one difference for D_1 and D_2, then we can get $\mathbf{q}_i^f-\tilde{\mathbf{q}}_i^f=2\sum_{f\in\mathcal{F}_i}S_{if}(\mathbf{u}_f-\tilde{\mathbf{u}}_f)$. Considering $|S_{if}-S'_{if}|\le 1$ and $||\mathbf{u}_f||\le 1$, it's obvious $||\mathbf{q}_i^f-\tilde{\mathbf{q}}_i^f||\le 2$.

We then formulate the probability that we get the same derived $\mathbf{U}$ with the different datasets D_1 and D_2. For each $\mathbf{u}_i$ of $\mathbf{U}$, we have

$$\begin{aligned}\frac{P[\mathbf{u}_i|D_1]}{P[\mathbf{u}_i|D_2]}=&\frac{\prod_{l\in\{1,2,...,K\}}p(q_{il}^f)}{\prod_{l\in\{1,2,...,K\}}p(\tilde{q}_{il}^f)}\\=&e^{-\frac{\epsilon\sum_l|q_{il}^f|}{2\Delta\sqrt{K}}}/e^{-\frac{\epsilon\sum_l|\tilde{q}_{il}^f|}{2\Delta\sqrt{K}}}=e^{\frac{\epsilon\sum_l(|q_{il}^f|-|\tilde{q}_{il}^f|)}{2\Delta\sqrt{K}}}\\\le&e^{\frac{\epsilon\sqrt{K\sum_l(q_{il}^f-\tilde{q}_{il}^f)^2}}{2\Delta\sqrt{K}}}=e^{\frac{\epsilon\sqrt{K}||\mathbf{q}_i^f-\tilde{\mathbf{q}}_i^f||}{2\Delta\sqrt{K}}}\le e^{\epsilon}\end{aligned}$$

So, we obtain the conclusion.

Proof of Theorem 3. We combine the rating model and social relation model together in Eq.(7). Since we don't jointly optimize Eq.(7) w.r.t. $\mathbf{V}$ and $\mathbf{U}$, we then optimize Eq.(7) w.r.t. $\mathbf{V}$ and $\mathbf{U}$ separately with Eq.(8) and Eq.(9).

For $\mathbf{V}$, the only difference of derivative of Eq.(5) and Eq.(8) w.r.t. $\mathbf{v}_j$ is the regularization $2\lambda\mathbf{v}_j$. Then we should add $2\lambda\mathbf{v}_j$ on both sides of Eq.(11). Since both datasets get the same $\mathbf{v}_j$, then the results won't change. The derived V still satisfies ϵ-differential privacy.

For $\mathbf{U}$, because of the difference of derivative and Eq.(6) and Eq.(9) w.r.t. $\mathbf{u}_i$, we need to add $2\sum_{j=1}^{m}\mathbf{I}_{ij}(\mathbf{u}_i^T\mathbf{v}_j-\mathbf{R}_{ij})\mathbf{v}_j+2\lambda\mathbf{u}_i$ on both sides of Eq.(12). Since D_1 and D_2 are only different at $\mathbf{u}_f$ and $\tilde{\mathbf{u}}_f$, then $||\mathbf{q}_i^f-\tilde{\mathbf{q}}_i^f||$ won't change, thus the derived U still satisfies ϵ-differential privacy.

In general, Algorithm 1 satisfies ϵ-differential privacy, which means attackers can't learn users' sensitive ratings or other user' latent profile in the whole process.