SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Efficient and secure outsourcing of bilinear pairings with single server

Min DONG & Yanli REN*

School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China

Appendix A Details about Q_1, Q_2, Q_3

$$\alpha_{j+1}\left(\prod_{\substack{b_mQ\in B_1\\ \sigma_m=+1}}\alpha_m\left(\prod_{\substack{b_mQ\in B_1\\ \sigma_m=-1}}\alpha_m\right)^{-1}\right)^{t_1}\left(\prod_{\substack{b_mQ\in B_{12}\\ \sigma_m=+1}}\alpha_m\left(\prod_{\substack{b_mQ\in B_{12}\\ \sigma_m=-1}}\alpha_m\right)^{-1}\right)^{t_2}\left(\prod_{\substack{b_mQ\in B_{13}\\ \sigma_m=+1}}\alpha_m\left(\prod_{\substack{b_mQ\in B_{13}\\ \sigma_m=-1}}\alpha_m\right)^{-1}\right)^{t_3}=Q_1$$

$$=\alpha_{j+2}\left(\prod_{\substack{b_mQ\in B_2\\ \sigma_m=+1}}\alpha_m\left(\prod_{\substack{b_mQ\in B_2\\ \sigma_m=-1}}\alpha_m\right)^{-1}\right)^{t_4}\left(\prod_{\substack{b_mQ\in B_{12}\\ \sigma_m=+1}}\alpha_m\left(\prod_{\substack{b_mQ\in B_{12}\\ \sigma_m=-1}}\alpha_m\right)^{-1}\right)^{t_5}\left(\prod_{\substack{b_mQ\in B_{23}\\ \sigma_m=+1}}\alpha_m\left(\prod_{\substack{b_mQ\in B_{23}\\ \sigma_m=-1}}\alpha_m\right)^{-1}\right)^{t_6},$$

$$\theta_1\left(\prod_{\substack{b_mQ\in B_3\\ \sigma_m=+1}}\alpha_m\left(\prod_{\substack{b_mQ\in B_3\\ \sigma_m=-1}}\alpha_m\right)^{-1}\right)^{t_7}\left(\prod_{\substack{b_mQ\in B_{13}\\ \sigma_m=+1}}\alpha_m\left(\prod_{\substack{b_mQ\in B_{13}\\ \sigma_m=-1}}\alpha_m\right)^{-1}\right)^{t_3}\left(\prod_{\substack{b_mQ\in B_{23}\\ \sigma_m=+1}}\alpha_m\left(\prod_{\substack{b_mQ\in B_{23}\\ \sigma_m=-1}}\alpha_m\right)^{-1}\right)^{t_6}$$

$$=\theta_2\left(\prod_{\substack{a_nP\in A_3\\ \rho_n=+1}}\beta_n\left(\prod_{\substack{a_nP\in A_3\\ \rho_n=-1}}\beta_n\right)^{-1}\right)^{t_7'}\left(\prod_{\substack{a_nP\in A_{13}\\ \rho_n=+1}}\beta_n\left(\prod_{\substack{a_nP\in A_{13}\\ \rho_n=-1}}\beta_n\right)^{-1}\right)^{t_3'}\left(\prod_{\substack{a_nP\in A_{23}\\ \rho_n=+1}}\beta_n\left(\prod_{\substack{a_nP\in A_{23}\\ \rho_n=-1}}\beta_n\right)^{-1}\right)^{t_6'}=Q_2,$$

$$\beta_{i+1}\left(\prod_{\substack{a_nP\in A_1\\ \rho_n=+1}}\beta_n\left(\prod_{\substack{a_nP\in A_1\\ \rho_n=-1}}\beta_n\right)^{-1}\right)^{t_1'}\left(\prod_{\substack{a_nP\in A_{12}\\ \rho_n=+1}}\beta_n\left(\prod_{\substack{a_nP\in A_{12}\\ \rho_n=-1}}\beta_n\right)^{-1}\right)^{t_2'}\left(\prod_{\substack{a_nP\in A_{13}\\ \rho_n=+1}}\beta_n\left(\prod_{\substack{a_nP\in A_{13}\\ \rho_n=-1}}\beta_n\right)^{-1}\right)^{t_3'}=Q_3,$$

$$=\beta_{i+2}\left(\prod_{\substack{a_nP\in A_2\\ \rho_n=+1}}\beta_n\left(\prod_{\substack{a_nP\in A_2\\ \rho_n=-1}}\beta_n\right)^{-1}\right)^{t_4'}\left(\prod_{\substack{a_nP\in A_{12}\\ \rho_n=+1}}\beta_n\left(\prod_{\substack{a_nP\in A_{12}\\ \rho_n=-1}}\beta_n\right)^{-1}\right)^{t_5'}\left(\prod_{\substack{a_nP\in A_{23}\\ \rho_n=+1}}\beta_n\left(\prod_{\substack{a_nP\in A_{23}\\ \rho_n=-1}}\beta_n\right)^{-1}\right)^{t_6'},$$

Appendix B Performance analysis

We analyze the privacy, efficiency and checkability of the proposed outsourcing algorithm here.

• **Privacy**

If the untrusted server wants to get useful information from inputs and outputs, there are some cases.

1. If the server wants to guess input A, it must know a_1P. From relationships among elements in *Rand*, we can know: probability of guessing the real ρ is $2^{-(i-1)}$; probability of guessing three of seven $t_u^{'}$ is s^{-3} where $u \in \{1, \cdots, 7\}$; and probability of guessing the distribution of $\beta_2 \cdots \beta_i$ in six sets is $6^{-(i-1)}$. So the total probability of guessing A is $\frac{1}{s^3 \cdot 12^{i-1}}$.

* Corresponding author (email: renyanli@shu.edu.cn)

2. Similarly, the probability of guessing B is about $\frac{1}{s^3 \cdot 12^{j-1}}$.

3. Briefly, the probability of guessing inputs for untrusted server is $\frac{1}{s^6 \cdot 12^{i-1} \cdot 12^{j-1}}$. If we set $s = 2, i = j = 10$, the probability is about 10^{-22}, even $s = 2, i = j = 5$, the probability is less than 10^{-10} .

- **Efficiency**

In the first proposed algorithm, outsourcer makes 1 call to *Rand* plus 4 point addition and $2i + 7s + 12$ multiplications to get $e(A, B)$. And it takes about $O(n)$ multiplications to compute single bilinear pairing. Thus, the algorithm (T, U) is an $O(\frac{1}{n})$-efficient implementation.

- **Checkability**

1. From the process of verifying, we can see the easiest way for server to cheat the client is that the server can guess which two are $\alpha_{j+1}, \alpha_{j+1}(\beta_{i+1}, \beta_{i+1})$ or θ_1, θ_2 in all queries correctly. The probability of guessing $\alpha_{j+1}, \alpha_{j+2}$ or β_{i+1}, β_{i+2} are $\frac{1}{(j+2)(j+1)}$ or $\frac{1}{(i+2)(i+1)}$, respectively; and the probability of guessing θ_1, θ_2 is $\frac{1}{(i+2)(j+2)}$.

2. The second way: server randomly chooses and changes two results to cheat the outsourcer. In order to pass the process of verifying, the server must guess two of $t_u(t_u^{'})$ or $\rho(\sigma)$, the probability is $\frac{1}{2} \cdot \frac{1}{2s} \cdot \frac{1}{2s} = 1/(8s^2)$.

3. Another difficult way is guessing $\rho(\sigma), t_u(t_u^{'})$ and distribution of the six sets, the probability is close to 0.

   So if the server is dishonest, errors will be detected with probability:

$$min\{1 - \frac{1}{(i+2)(i+1)}, 1 - \frac{1}{(8s^2)}\}.$$

   If we also set $s = 2, i = j = 10$, we can get that the checkability is $\frac{31}{32} (\approx 0.9688)$.

Appendix C Details about Q_4, Q_5, Q_6

$$\prod_{y=1}^{t} \alpha_{y(j+1)} \left(\prod_{\substack{y=1 \\ b_m Q \in B_1 \\ \sigma_m = +1}}^{t} \alpha_{ym} \left(\prod_{\substack{y=1 \\ b_m Q \in B_1 \\ \sigma_m = -1}}^{t} \alpha_{ym} \right)^{-1} \right)^{t_1} \left(\prod_{\substack{y=1 \\ b_m Q \in B_{12} \\ \sigma_m = +1}}^{t} \alpha_{ym} \left(\prod_{\substack{y=1 \\ b_m Q \in B_{12} \\ \sigma_m = -1}}^{t} \alpha_{ym} \right)^{-1} \right)^{t_2}$$
$$\cdot \left(\prod_{\substack{y=1 \\ b_m Q \in B_{13} \\ \sigma_m = +1}}^{t} \alpha_{ym} \left(\prod_{\substack{y=1 \\ b_m Q \in B_{13} \\ \sigma_m = -1}}^{t} \alpha_{ym} \right)^{-1} \right)^{t_3} = Q_4$$
$$= \prod_{y=1}^{t} \alpha_{y(j+2)} \left(\prod_{\substack{y=1 \\ b_m Q \in B_2 \\ \sigma_m = +1}}^{t} \alpha_{ym} \left(\prod_{\substack{y=1 \\ b_m Q \in B_2 \\ \sigma_m = -1}}^{t} \alpha_{ym} \right)^{-1} \right)^{t_4} \left(\prod_{\substack{y=1 \\ b_m Q \in B_{12} \\ \sigma_m = +1}}^{t} \alpha_{ym} \left(\prod_{\substack{y=1 \\ b_m Q \in B_{12} \\ \sigma_m = -1}}^{t} \alpha_{ym} \right)^{-1} \right)^{t_5}$$
$$\cdot \left(\prod_{\substack{y=1 \\ b_m Q \in B_{23} \\ \sigma_m = +1}}^{t} \alpha_{ym} \left(\prod_{\substack{y=1 \\ b_m Q \in B_{23} \\ \sigma_m = -1}}^{t} \alpha_{ym} \right)^{-1} \right)^{t_6}$$

$$\prod_{y=1}^{t} \theta_{y1} \left(\prod_{\substack{y=1 \\ b_m Q \in B_3 \\ \sigma_m = +1}}^{t} \alpha_{ym} \left(\prod_{\substack{y=1 \\ b_m Q \in B_3 \\ \sigma_m = -1}}^{t} \alpha_{ym} \right)^{-1} \right)^{t_7} \left(\prod_{\substack{y=1 \\ b_m Q \in B_{13} \\ \sigma_m = +1}}^{t} \alpha_{ym} \left(\prod_{\substack{y=1 \\ b_m Q \in B_{13} \\ \sigma_m = -1}}^{t} \alpha_{ym} \right)^{-1} \right)^{t_3}$$
$$\cdot \left(\prod_{\substack{y=1 \\ b_m Q \in B_{23} \\ \sigma_m = +1}}^{t} \alpha_{ym} \left(\prod_{\substack{y=1 \\ b_m Q \in B_{23} \\ \sigma_m = -1}}^{t} \alpha_{ym} \right)^{-1} \right)^{t_6} = Q_5$$

$$= \prod_{y=1}^{t} \theta_{y2} \left(\prod_{\substack{y=1 \\ a_n P \in A_3 \\ \rho_n = +1}}^{t} \beta_{yn} \left(\prod_{\substack{y=1 \\ a_n P \in A_3 \\ \rho_n = -1}}^{t} \beta_{yn} \right)^{-1} \right)^{t_7'} \left(\prod_{\substack{y=1 \\ a_n P \in A_{13} \\ \rho_n = +1}}^{t} \beta_{yn} \left(\prod_{\substack{y=1 \\ a_n P \in A_{13} \\ \rho_n = -1}}^{t} \beta_{yn} \right)^{-1} \right)^{t_3'}$$

$$\cdot \left(\prod_{\substack{y=1 \\ a_n P \in A_{23} \\ \rho_n = +1}}^{t} \beta_{yn} \left(\prod_{\substack{y=1 \\ a_n P \in A_{23} \\ \rho_n = -1}}^{t} \beta_{yn} \right)^{-1} \right)^{t_6'}$$

$$\prod_{y=1}^{t} \beta_{y(i+1)} \left(\prod_{\substack{y=1 \\ a_n P \in A_1 \\ \rho_n = +1}}^{t} \beta_{yn} \left(\prod_{\substack{y=1 \\ a_n P \in A_1 \\ \rho_n = -1}}^{t} \beta_{yn} \right)^{-1} \right)^{t_1'} \left(\prod_{\substack{y=1 \\ a_n P \in A_{12} \\ \rho_n = +1}}^{t} \beta_{yn} \left(\prod_{\substack{y=1 \\ a_n P \in A_{12} \\ \rho_n = -1}}^{t} \beta_{yn} \right)^{-1} \right)^{t_2'}$$

$$\cdot \left(\prod_{\substack{y=1 \\ a_n P \in A_{13} \\ \rho_n = +1}}^{t} \beta_{yn} \left(\prod_{\substack{y=1 \\ a_n P \in A_{13} \\ \rho_n = -1}}^{t} \beta_{yn} \right)^{-1} \right)^{t_3'} = Q_6$$

$$= \prod_{y=1}^{t} \beta_{y(i+2)} \left(\prod_{\substack{y=1 \\ a_n P \in A_2 \\ \rho_n = +1}}^{t} \beta_{yn} \left(\prod_{\substack{y=1 \\ a_n P \in A_2 \\ \rho_n = -1}}^{t} \beta_{yn} \right)^{-1} \right)^{t_4'} \left(\prod_{\substack{y=1 \\ a_n P \in A_{12} \\ \rho_n = +1}}^{t} \beta_{yn} \left(\prod_{\substack{y=1 \\ a_n P \in A_{12} \\ \rho_n = -1}}^{t} \beta_{yn} \right)^{-1} \right)^{t_5'}$$

$$\cdot \left(\prod_{\substack{y=1 \\ a_n P \in A_{23} \\ \rho_n = +1}}^{t} \beta_{yn} \left(\prod_{\substack{y=1 \\ a_n P \in A_{23} \\ \rho_n = -1}}^{t} \beta_{yn} \right)^{-1} \right)^{t_6'}$$