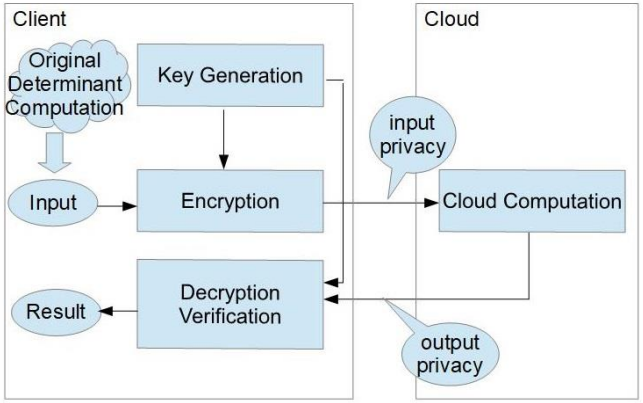
Secure outsourcing of large matrix determinant computation

Jiayang LIU, Jingguo BI, Mu LI

Frontiers of Computer Science, DOI: 10.1007/s11704-019-9189-7

Problems & Ideas

- Problems: a secure outsourcing method for large matrix determinant computation
  - Correctness
  - Security
  - Efficiency
  - Robust cheating resistance
- Ideas: reduce the local computational workloads and outsource the determinant computation
  - permutation and mix-row/mix-column operations
  - Main part of encryption: $Y=P1 \cdot X \cdot P2$



Main Contributions

- Encryption

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} \beta_3(\alpha_2(a_{23}+a_{43})+\alpha_2(a_{24}+a_{44})) & \beta_1(\alpha_2(a_{21}+a_{41})+\alpha_2(a_{22}+a_{42})) & \beta_4\alpha_2(a_{24}+a_{44}) & \beta_2(\alpha_2(a_{22}+a_{42})+\alpha_2(a_{23}+a_{43})) \\ \beta_3(\alpha_4a_{43}+\alpha_4a_{44}) & \beta_1(\alpha_4a_{41}+\alpha_4a_{42}) & \beta_4\alpha_4a_{44} & \beta_2(\alpha_4a_{42}+\alpha_4a_{43}) \\ \beta_3(\alpha_1(a_{13}+a_{33})+\alpha_1(a_{14}+a_{34})) & \beta_1(\alpha_1(a_{11}+a_{31})+\alpha_1(a_{12}+a_{32})) & \beta_4\alpha_1(a_{14}+a_{34}) & \beta_2(\alpha_1(a_{12}+a_{32})+\alpha_1(a_{13}+a_{33})) \\ \beta_3(\alpha_3(a_{33}+a_{43})+\alpha_3(a_{34}+a_{44})) & \beta_1(\alpha_3(a_{31}+a_{41})+\alpha_3(a_{32}+a_{42})) & \beta_4\alpha_3(a_{34}+a_{44}) & \beta_2(\alpha_3(a_{32}+a_{42})+\alpha_3(a_{33}+a_{43})) \end{pmatrix}$$

- **Experimental Results and Comparison**

Table 1: Experimental Results (SetPrecision(100))

	Our Algorithm					
n	Original	Cloud	Client	AS	CE	Extra cost
2000	559.1	558.5	38.5	14.5	1.00	0.07
3000	1920.8	1911.3	87.5	22.0	1.00	0.04
4000	4545.1	4527.3	154.3	29.5	1.00	0.03
5000	8778.1	8744.4	244.6	35.9	1.00	0.02
	Lei's Algorithm $m = 200$					
2000	558.9	664.6	30.7	18.2	0.84	0.24
3000	1913.8	2152.9	66.8	28.6	0.89	0.16
4000	4491.7	4900.9	115.9	38.8	0.92	0.12
5000	8844.5	9493.2	179.9	49.2	0.93	0.09