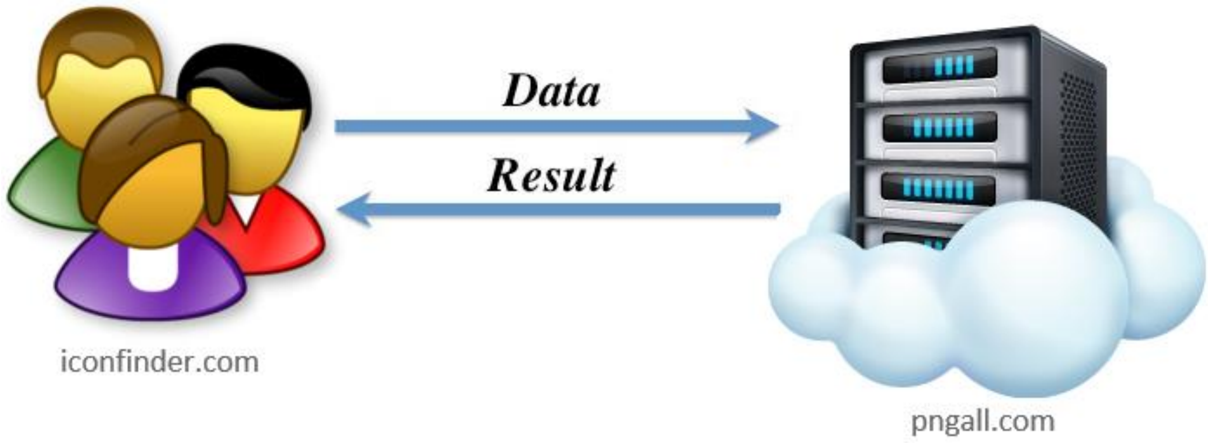
A Game-Theoretic Model for Outsourced Computation Verification

Balazs Pejo and Qiang Tang *(name.surname@uni.lu)*

Introduction

Companies collect data to provide better services. Processing these data is computationally intense, making it infeasible for companies without the necesarry resources. A natural solution is outsourcing:



Via outsourcing, the integrity of the result can be harmed. However, it can be guaranteed using economic approaches to create incentives for honest behaviors.

Payoff Matrix

		IN	OUT
Full Detect (P_A)	Server	Ψ	- (1 – ρ) - $F_\phi(\rho)$
	Client	1 + b + $F_\phi(\rho)$	- $\kappa_b(\rho)$ – ψ - V(σ)
Detect (1-P_A-P_0)	Server	Ψ	- (1 – ρ)
	Client	1 + b	- $\kappa_b(\rho)$ – ψ - V(σ)
Not Detect (P_0)	Server	1 + w	- (1 – ρ)
	Client	1 + b	- $\lambda_b(\rho)$ - (1 + w) - V(σ)

The client has to have the highest payoff when no cheating occurs

$$U_C(w,\psi,\sigma,\rho) \le U_C(w,\psi,\sigma,0) \text{ for all } \rho$$

The client wants the server not to cheat on more than θ

$$U_S(w,\psi,\sigma,\rho) \le U_S(w,\psi,\sigma,\theta) \text{ for all } \theta \le \rho$$

Using these conditions, two Stackelberg games are defined, depending on who makes the offer (w.Ψ).

Parameters

Name	Meaning
ρ	Cheating rate (0 ≤ ρ ≤ 1)
σ	Checking rate (0 ≤ σ ≤ 1)
K	Number of outputs / results
C	Cost of computation (C = 1)
ψ	Deposit (0 ≤ ψ ≤ 1)
W	Payment (0 < W = 1 + w)
B	Benefit of the results (W < B = 1 + b)
θ	Tolerated cheating rate (0 ≤ θ ≤ 1)
ϕ	Punished cheating rate (0 ≤ ϕ ≤ 1)
$P_0(K,\sigma,\rho)$	Probability of no detection
$P_A(K,\sigma,\rho)$	Probability of full detection
$F_\phi(\rho)$	Fine (0 ≤ f)
V(σ)	Verification cost
$\kappa_b(\rho)$	Known benefit reducer (0 ≤ κ)
$\lambda_b(\rho)$	Unknown benefit reducer (κ ≤ λ)

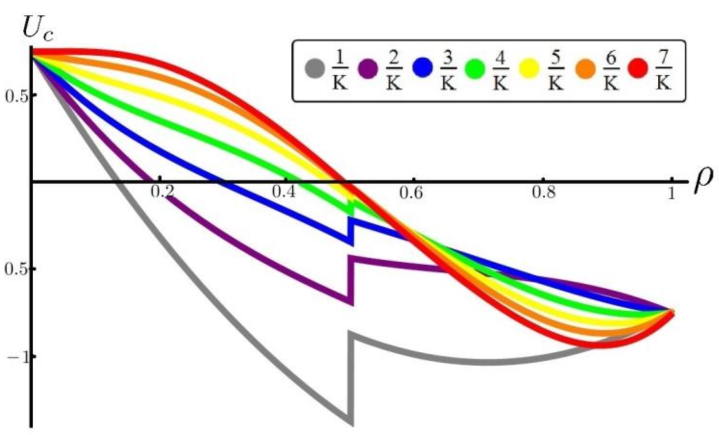
Predetermined variables: K, C, B, θ, ϕ, F, V, κ, λ
Free variables: W, ψ, σ, ρ
$F_\phi(\rho)$ = f if ϕ ≤ ρ and 0 otherwise

$$P_0(K,\sigma,\rho) = \frac{\binom{(1-\rho)K}{\sigma K}}{\binom{K}{\sigma K}} \qquad P_A(K,\sigma,\rho) = \frac{\binom{\rho K}{\sigma K}}{\binom{K}{\sigma K}}$$

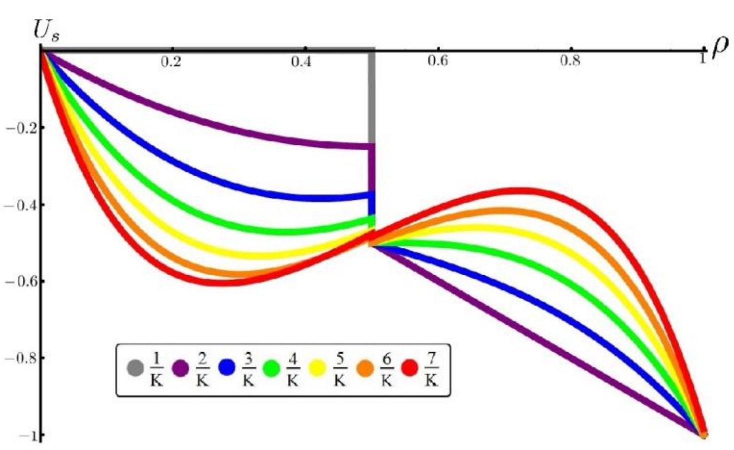
Conclusion

- The client prefers high σ.
- The server prefers low σ.
- σ should always be higher than 1/K.
- Besides the client, the server also prefers low tolerated cheating rates.
- Independent from θ, the server's dominant strategy is *not cheat*.
- The leading player has overpowering adventage, the follower usually gains the minimum.

Example: Client is the leader



Server's Payoff



Client's Payoff

K	=	1 000 000
B	=	0.75
θ	=	0.05
ϕ	=	0.5
f	=	1
V(σ)	=	σ
$\kappa_b(\rho)$	=	2 (1+b) ρ
$\lambda_b(\rho)$	=	4 (1+b) ρ

University of Luxembourg · SnT · JFK Building · 29, avenue John F. Kennedy · L-1855 Luxembourg · Tel. +352 /46 66 44 -5721 · snt@uni.lu · www.securityandtrust.lu