

Contractual Anonymity

Edward J. Schwartz, David Brumley, Jonathan M. McCune

Goals

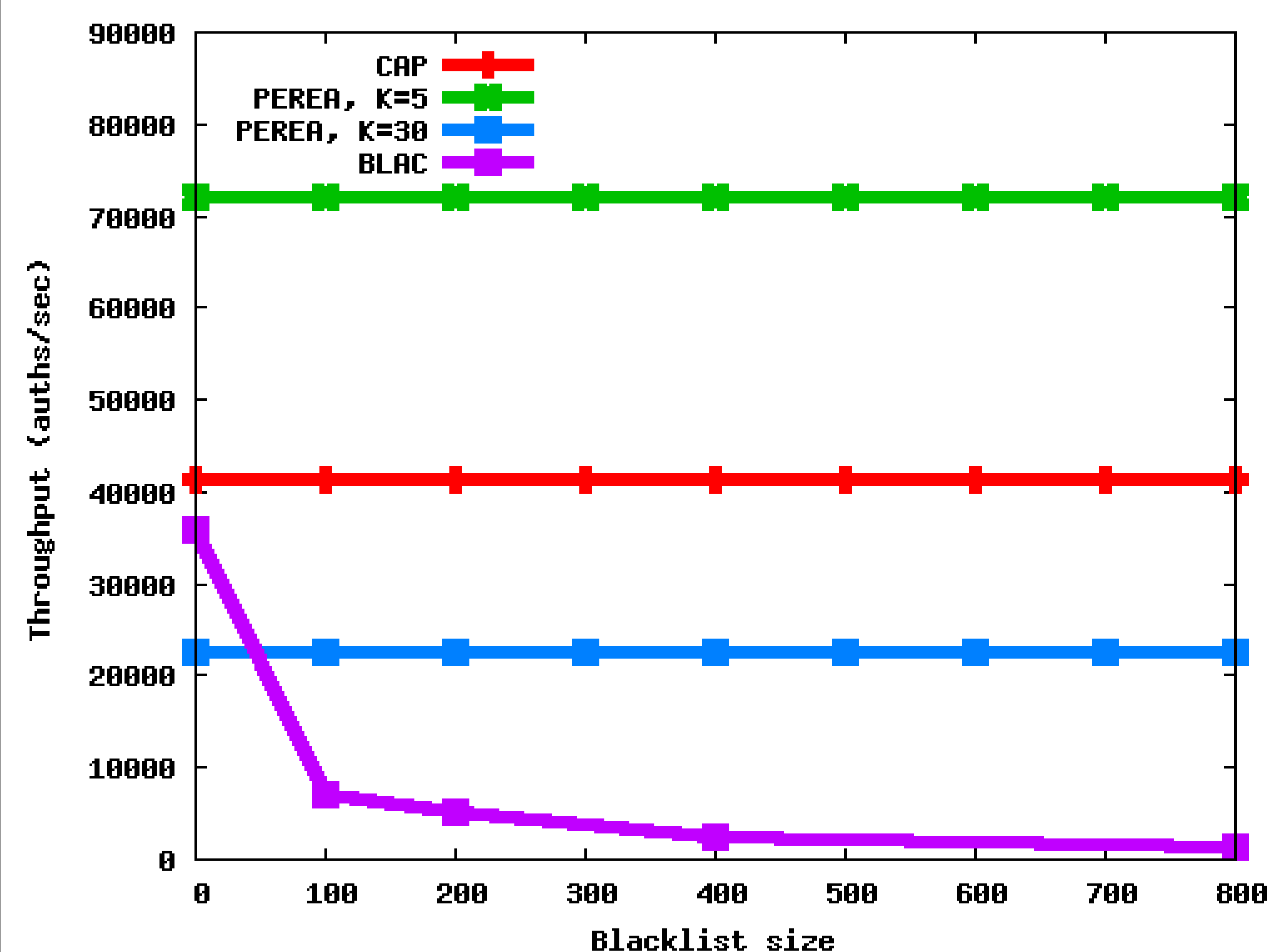
- Some network services can benefit from user **anonymity**
 - E.g., support forums for patients of terminal diseases, or victims of serious crimes
- Service providers need some level of **accountability**
 - How can misbehaving users be stopped if they are completely anonymous?
- Well-behaved users should be **guaranteed anonymity**
- Service providers should be **guaranteed** the ability to **blacklist** misbehaving users
- Users and service providers must both **agree on a contract** that specifies good behavior
- Contract guarantees that **user can not be discriminated against** unless she breaks her contract

Approach

- Use **verifiable third party (VTP)** to manage identities
 - Users and service providers can verify VTP implementation properties by using **trusted computing**
 - VTP runs in **hardware-assisted isolation**; not affected by OS or BIOS compromise
- Unique certificates distributed with each TPM can serve as a **unique identity for users**
- Contract consists of **flexible policies**
- Users are bound to **group signature group**
 - Provides **anonymity and unlinkability** among members of the group
 - VTP acts as **group manager**, can deanonymize users when they break contract
- Once user obtains credentials, **authenticating is fast!**
 - One group signature operation for user
 - One group verification operation for service

Efficient Implementation

- Our system, CAP, is comparable to prior work on the SP



Better

- CAP scales better than prior work on the user

