09/25/2013

GMW vs. Yao

- preprocessing ?
  * GMW:
    preprocess all OTs
    Online phase:
    - does not involve any crypto
    - has low communication
    drawback:
    - round complexity linear in circuit depth
    overall computation:
    - 1 OT per gate
    - 4-in-1 H-evaluations per gate
      (using load-balancing)

  * Yao:
    preprocessing
    - preprocess OTs
    - (preprocess garbled-circuit generation)
    online phase:
    - garbled-circuit evaluation
    - GC generation
    ⇒ high communication
    round-complexity constant
    overall computation:
    - cost of generating / evaluating garbled gates
    - 3-in-1 AES operations per gate

Semi-honest 2PC implementations:

- Fairplay (2004)
  - Yao
- Tasty (2010)
  - mixed-mode protocols
  - Yao or homomorphic encryption
- Huang et al. (2011)
  - pipelining
  - significantly more efficient / scalable
  - prog. framework
  - Yao
- Choi et al.
  - GMW
- Schneider-Zohner (2013)
  - GMW vs. Yao

TASTY

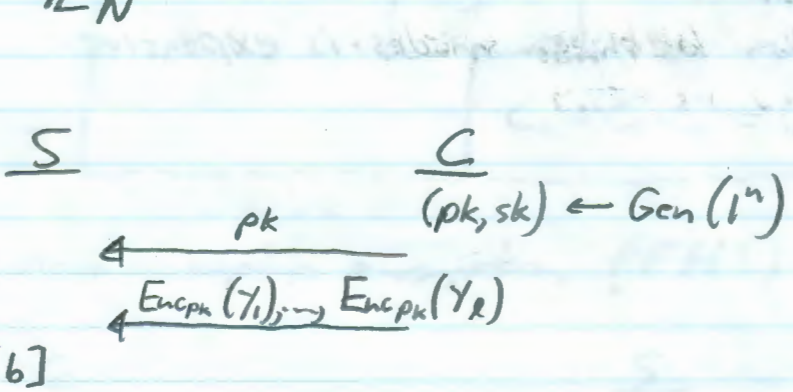
hom. enc:

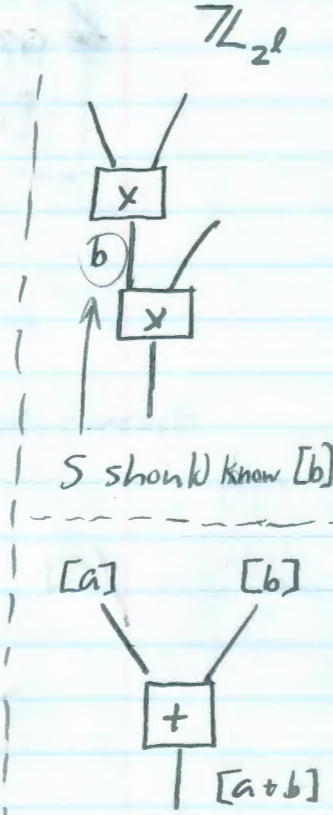
given encryption of a, b,
can generate encryption of $a+b$

$[a], [b] \Rightarrow [a+b]$

$[a], r \Rightarrow [r \cdot a]$

Paillier encryption scheme is homomorphic over $\mathbb{Z}_N$





S

C

$\tilde{x}$: garbled output value

$\tilde{x} = [(k_1, \lambda_1), \ldots, (k_\ell, \lambda_\ell)]$

$\leftarrow \text{Enc}_{pk}(\lambda_1), \ldots$

For all i {

If $\pi_i = 0$

randomize C_i

if $\pi_i = 1$

$C_i = C_i^{-1}$

}

output $[x] = \prod_{i=1}^{\ell} C_i^{2^i}$

* conversion between modes is expensive