Distributed Paillier Cryptosystem without Trusted Dealer

Takashi Nishide

Kyushu University

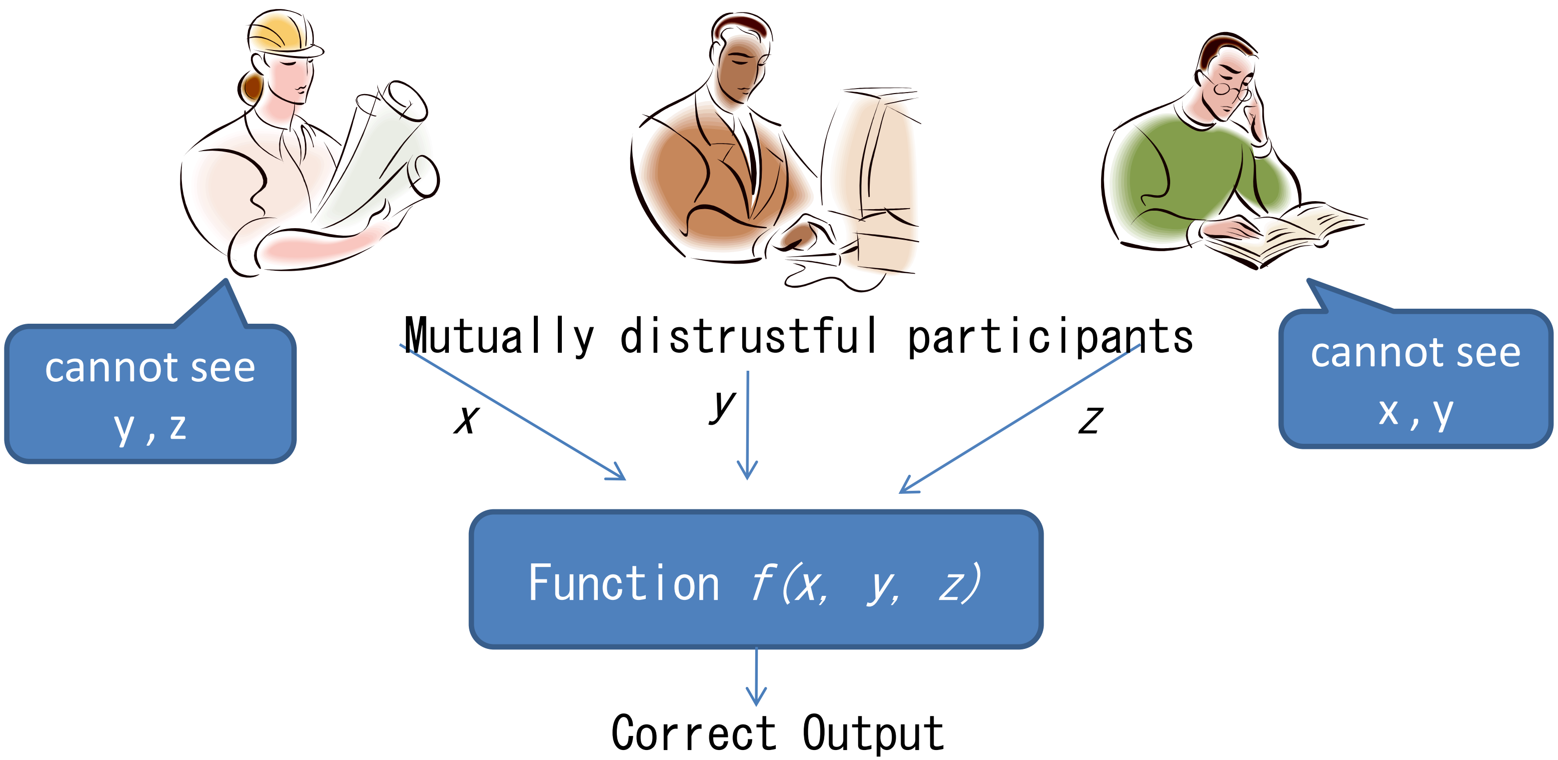
Kouichi Sakurai

Kyushu University

August 25th, 2010

Supported by JAPAN SCIECE AND TECHNOLOGY AGENCY (JST), Strategic Japanese-Indian Cooperative Programme on Multidisciplinary Research Field, which combines Information and Communications Technology with Other Fields, entitled "Analysis of Cryptographic Algorithms and Evaluation on Enhancing Network Security Based on Mathematical Science."

Multiparty Computation(MPC)



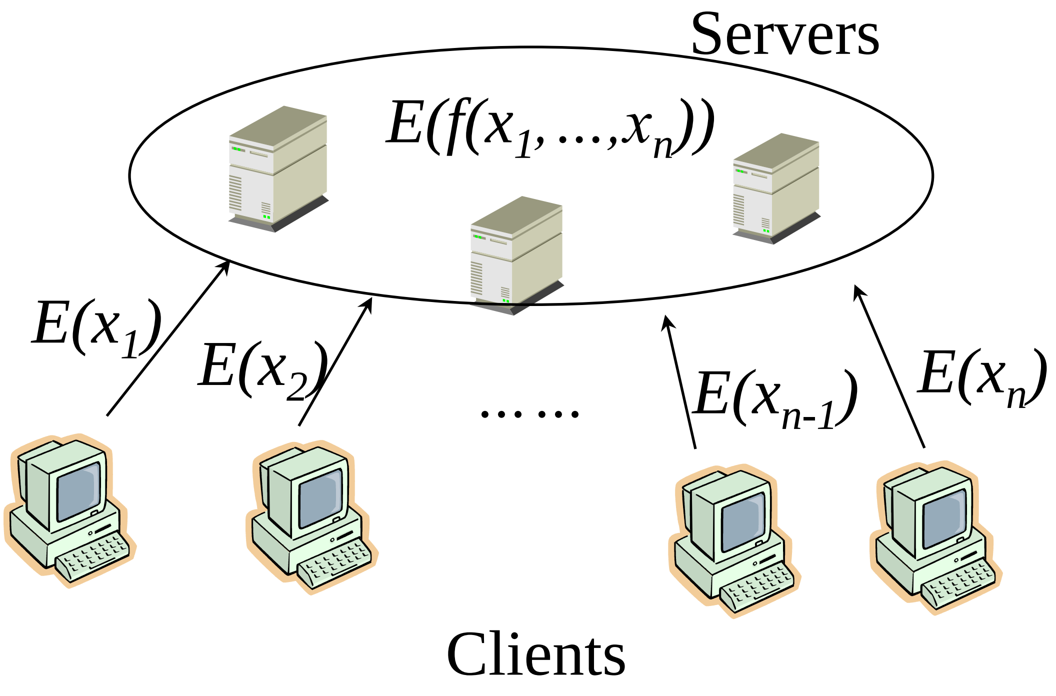
- Applications
  - Electronic Voting $f(x_1, \ldots, x_n) = \sum x_i$
  - Electronic Auction $f(x_1, \ldots, x_n) = \max(x_1, \ldots, x_n)$
  - Privacy Preserving Data Mining, etc

Two Major Approaches to MPC

- Shamir's Secret Sharing
  - Secrets are shared among the participants
- Threshold Homomorphic Cryptosystem (THC)
  - special public key cryptosystem
  - Secrets are encrypted
  - Homomorphic property
    - $E(m_1) * E(m_2) = E(m_1 + m_2)$
    - $E(m)^k = E(km)$

MPC Based on THC

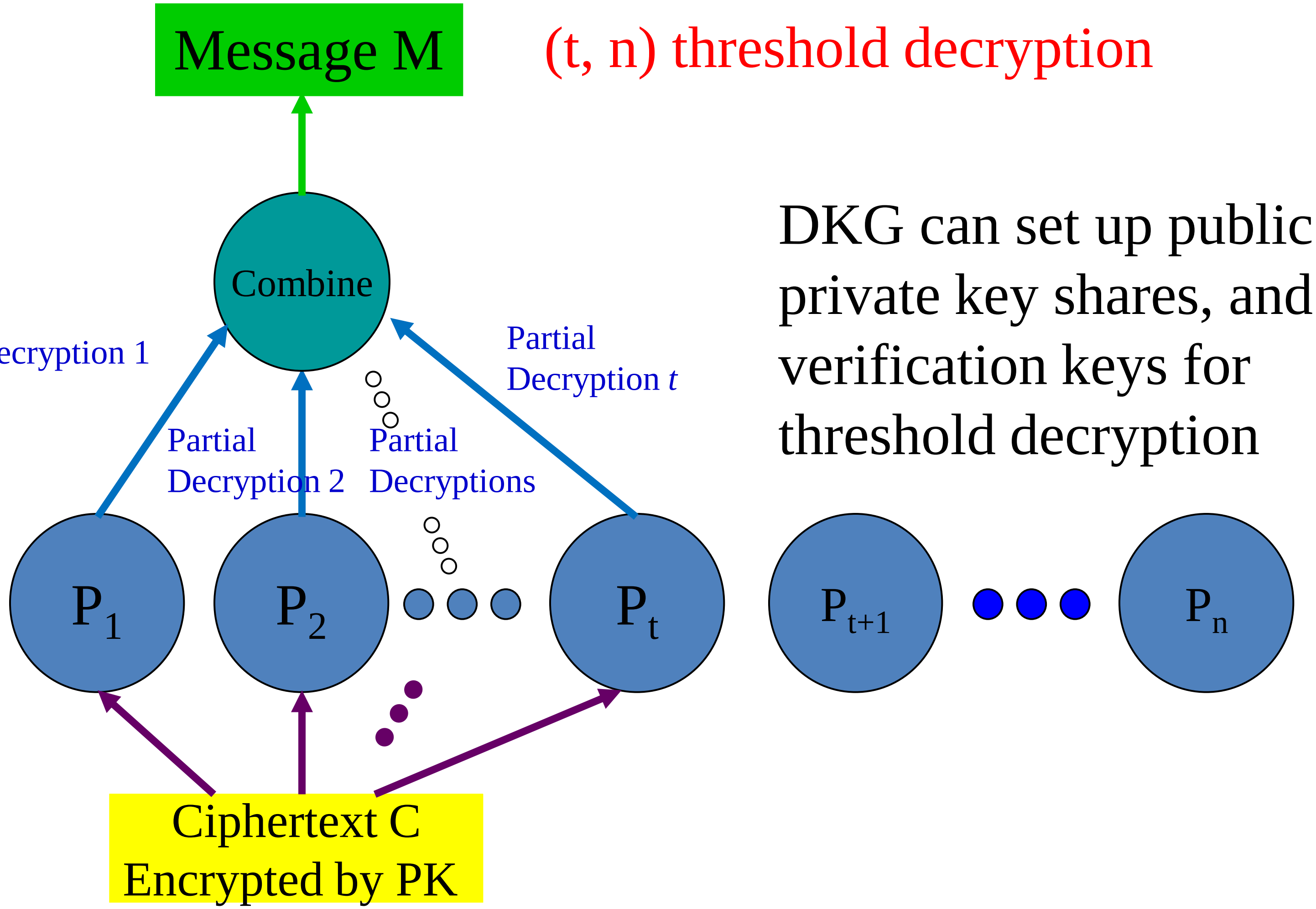
- Client-Server Model
  - Many clients provide encrypted data as inputs
  - Servers do blinded computation on encrypted data using homomorphic property



Initial Key Setup for THC

- In the initial key setup
  - the private decryption key must be shared among the participants
  - Verification keys must also be established for robustness against misbehaving participants
- The key setup can be done
  - by a trusted party
    - Single point of attack
  - by MPC again w/o trusted party (dealer)
    - Called Distributed Key Generation (DKG)

Key Setup & Threshold Decryption



(t, n) threshold decryption

DKG can set up public key, private key shares, and verification keys for threshold decryption

Popular Homomorphic Crypto

- ElGamal
  - Simple & robust DKG w/o trusted dealer
  - Additively homomorphic ElGamal can support only small plaintext space
- Paillier
  - Complex DKG or trusted dealer
    - Robust DKG w/o trusted setup (CRS) is non-trivial
  - Paillier can support huge plaintext space
  - Building block for many cryptographic protocols
    - meaningful to eliminate trusted dealer of private key to avoid a single point of attack

Related Work

- [BF97] realized first DKG for RSA in honest-but-curious model (i.e., non-robust)
  - Paillier cryptosystem also needs RSA modulus, so part of [BF97] can be used in DKG for Paillier
- [FMY98] extended [BF97] with robustness techniques
  - We use the different robustness techniques
  - The private key of Paillier is different from that of RSA , so we need to construct a different robust protocol

Related Work (Cont'd)

- [DK01] proposed threshold RSA signature using non-safe prime product with non-standard but reasonable assumption
  - We extend the assumption to Paillier setting to construct an efficient zero-knowledge proof for partial decryption share
- [DM10] proposed a novel distributed primality test in DKG for RSA
  - the protocol is designed only for three parties
  - needs a trusted setup (CRS for commitment)

Properties of Our Construction

- Based on [FPS00]
  - it assumes that a trusted dealer generates a safe safe prime product for RSA modulus
  - We do not need a safe prime product with additional assumption
- Robust protocol
- No trusted setup such as CRS
- Efficient ZKP for partial decryption share with non-binary challenge set
- Light range proof for shared secrets

Avoiding Safe Primes

- [FPS00] needs safe prime product where N = pq, p = 2p'+1, q = 2q'+1
  - But generating such N by DKG can be time-consuming though not impossible…
  - This condition is necessary for efficient proof of equality mod N
- We apply the assumption [DK01] to Paillier setting
  - Informally the assumption says that given N, p-1 (or q-1) includes a large prime factor Q such that it is infeasible to guess Q and 1/Q is negligible

Light Range Proof

- In [BF97], N is computed as
  - $N = (p_1 + p_2 + \ldots + p_n)(q_1 + q_2 + \ldots + q_n)$
  - p_i, q_i are chosen by participant P_i
- We need zero-knowledge proof that p_i, q_i are in the appropriate range $[2^{k-1}, 2^k - 1]$
  - classical bitwise range proof is inefficient for large numbers [Mao98]
  - [BCDG87] can be used with a group of known prime order where the expansion rate is 3, i.e., $p_i, q_i \in [0, 3*2^{k-1}]$

Sharing Private Key Robustly

- In our construction, $\varphi(N) = (p-1)(q-1)$ is shared over a prime field.
- the following values must be computed to share key
  - $\theta = \beta\varphi \bmod N$ revealed where β is a shared random secret
  - $\beta\varphi$ is shared over the integers
- We compute and reveal $\theta' = \beta\varphi + NR$ robustly
  - where R is a shared random secret over the integers
  - $\theta = \theta' \bmod N$
  - Sharing of $\beta\varphi$ obtained from sharing of $\theta' - NR$ over the integers where θ' and N are public values
  - can prove that θ' is indistinguishable from $\beta(N-1) + NR$
- Trial division on p,q can be done robustly in a similar way

Summary

- Constructed a distributed key generation protocol for Paillier cryptosystem based on [FPS00]
- DKG with Robustness
- No need to generate safe prime product
- No need for trusted setup
- Non-standard but reasonable assumption from [DK01] to realize efficient ZKP mod N

Thank you for you attention!