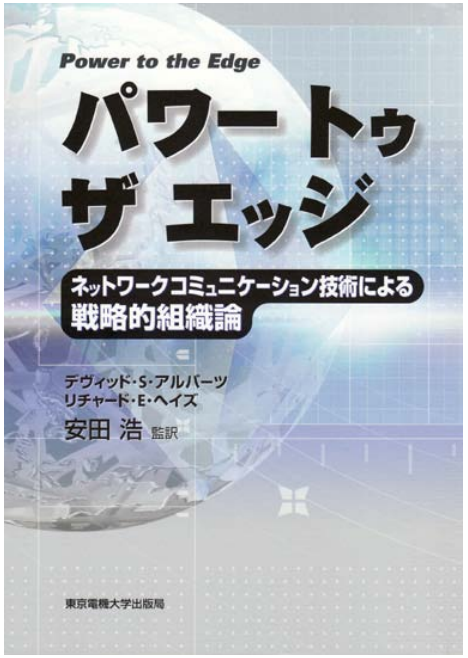
Privacy Preserving Service Discovery for Interoperability in "Power to the Edge" Approach

Research and Development Initiative,
Chuo University

Hiroshi Yamaguchi, Masahito Gotaishi,
Shigeo Tsujii, Norihisa Doi

“Power to the Edge” Approach for the non-Military Activity

- Masahito Gotaishi,
  - A member of the Japanese Translation team of “Power to the Edge”
  - Long for the application of “Power to the Edge” approach to Medicine and Care
- Hiroshi Yamaguchi
  - Once presented in ICCRTS (2009)
  - Application of PTE to control the performance of Orchestra
  - Best Paper of the Section



Problem to Solve

- Information is necessary in “Self-Synchronization” and “Shared Situation Awareness”
- Information is shared in the organization
- Typically information is shared with the partners
- These information are internal ones and often **Confidential**

Examples in the Real World

- e-Administration: Taxing, refund of high medical charge, allowance for female-headed household, etc.
  - Information is not widely shared within the public administration office
  - because it is “Personal Information”
- Medicine & Care: Making use of the chart data, result of the treatment, etc.
  - Strictly confidential
  - But medicine needs the data

Dilemma

- “Value” of the Information is realized ONLY WHEN it is used
- Usually solved by "Trade-Off."
- Is there a "Best of the Both World" solution ?

Our Proposal (medicine & care)

- Clinical data computed while they are encrypted (secret sharing) -assuming cloud computing
- Protecting the search operation information, while enabling semantic search
- Anonymous Feedback
- Access Control using Cryptosystem

Privacy Preserving Data Processing (PPDP)

Encrypted Medical Information DB (Personal Information)

Proof of validity Protocol

PPDP is correctly Processed (i.e. Personal Information Is not revealed)?

Privacy Preserving Data Processing

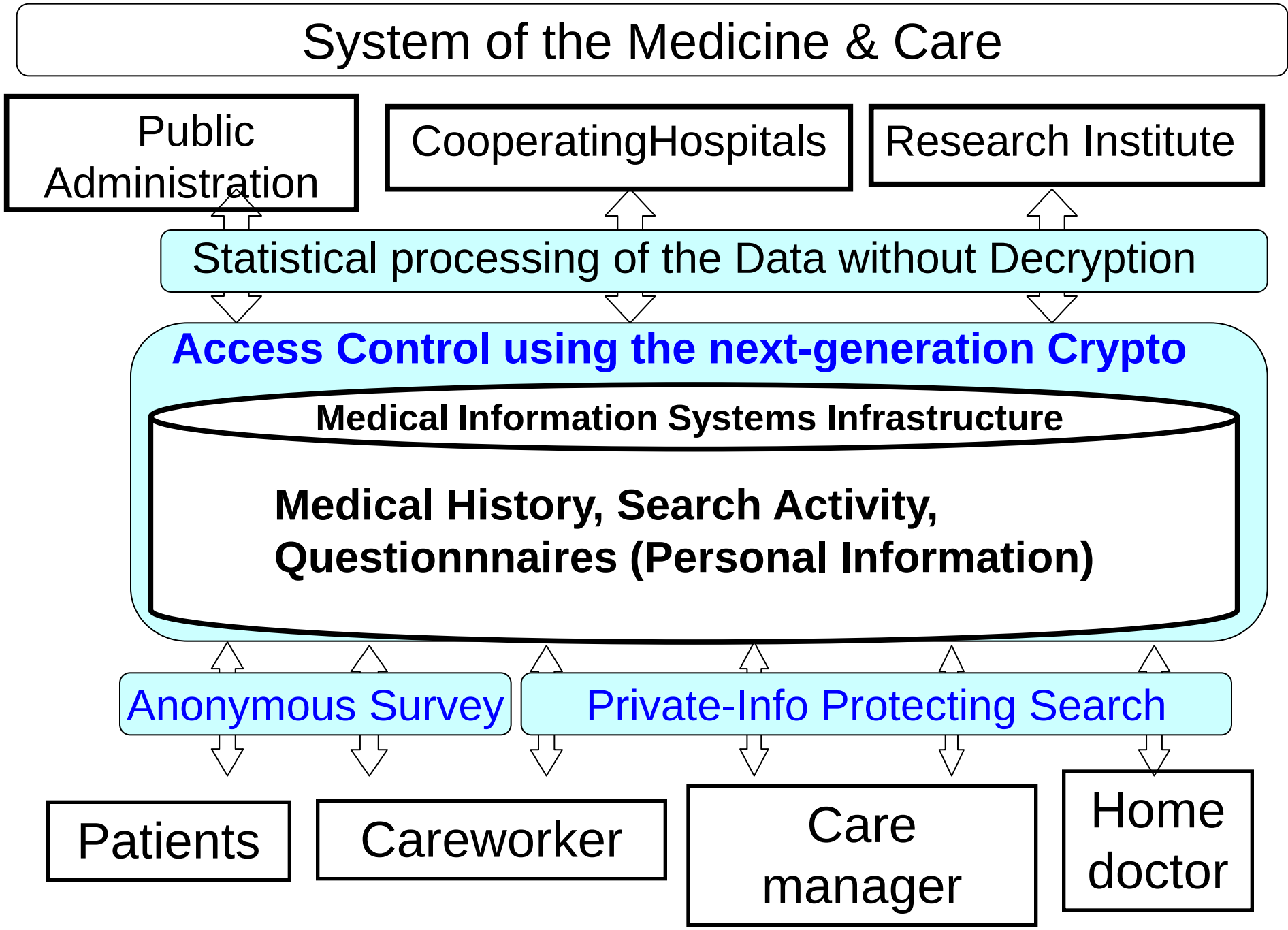
Functional Operation (∑,∏ etc.) ,while encrypted

Data Processing (Statistics, Mining etc.)

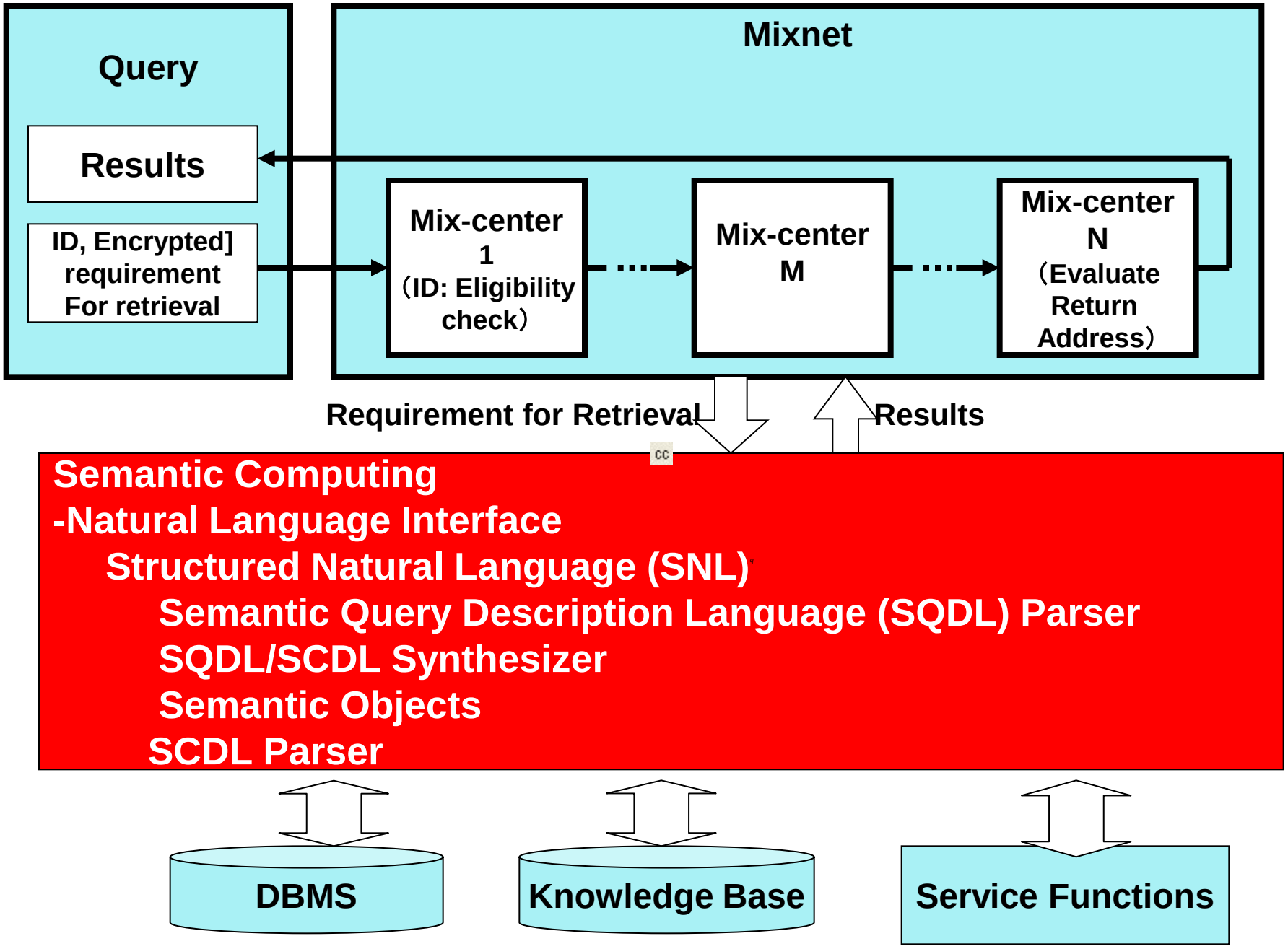
Semantic Computing (Natural Language, etc.)

Patients are able to confirm that their privacy are preserved. ‘Relieved!’

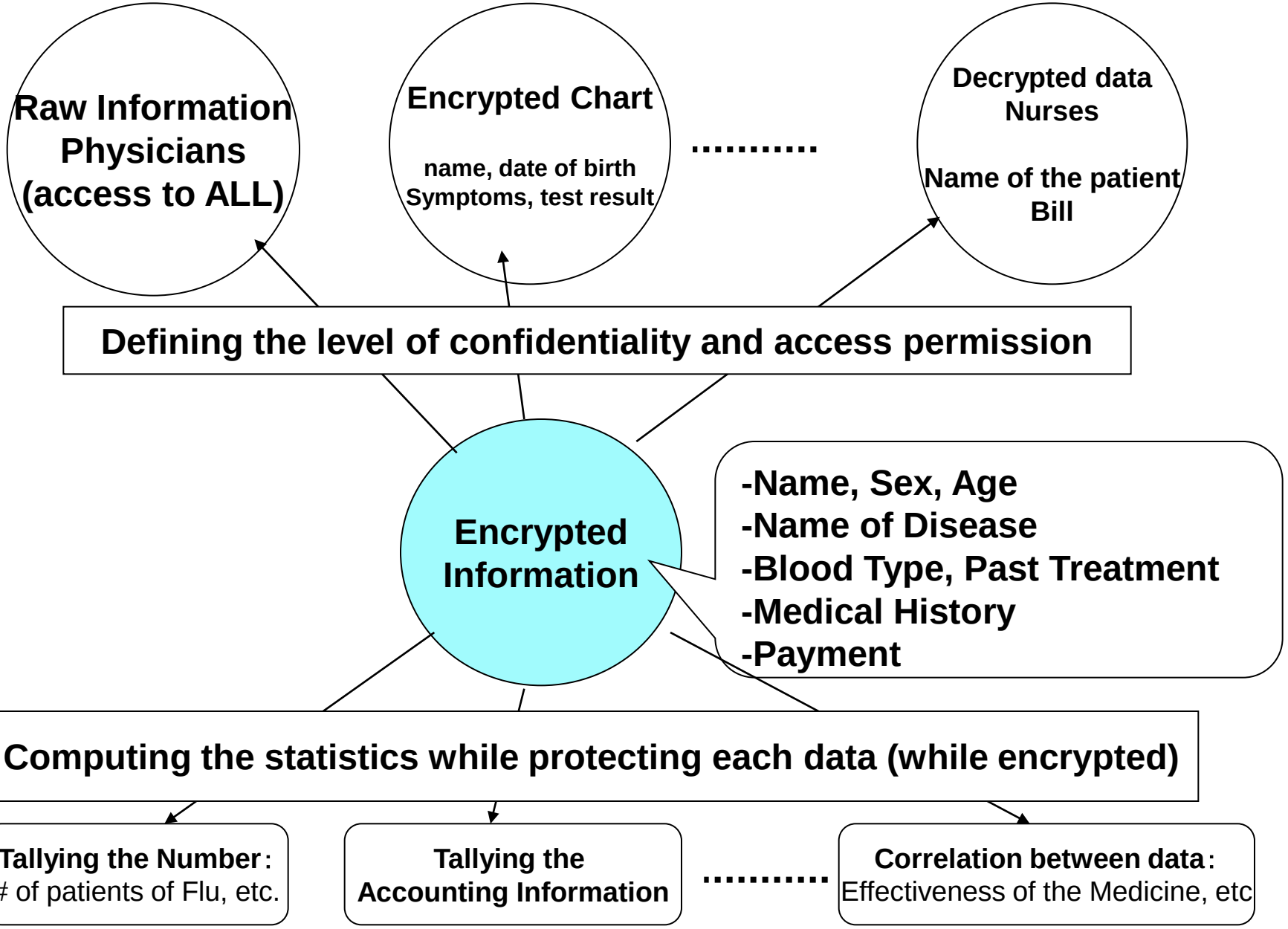
Medical researchers are able to obtain processed data without decrypting the encrypted data


System of the Medicine & Care
Public Administration
CooperatingHospitals
Research Institute
Statistical processing of the Data without Decryption
Access Control using the next-generation Crypto
Medical Information Systems Infrastructure
Medical History, Search Activity,
Questionnnaires (Personal Information)
Anonymous Survey
Private-Info Protecting Search
Patients
Careworker
Care manager
Home doctor

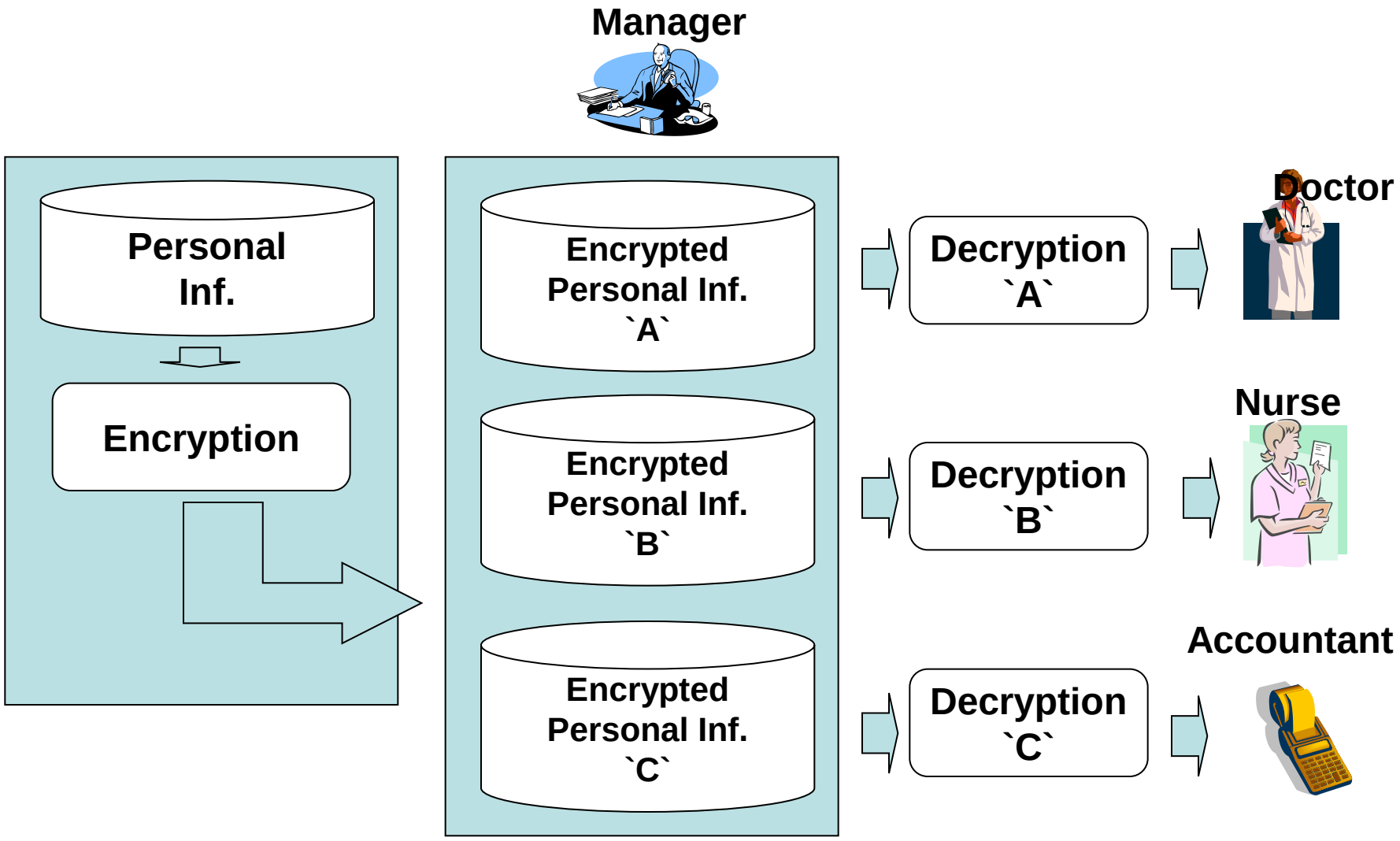
Private Information Retrieval including Content-based Multimedia Inf.



Access Control / Operation without Decryption

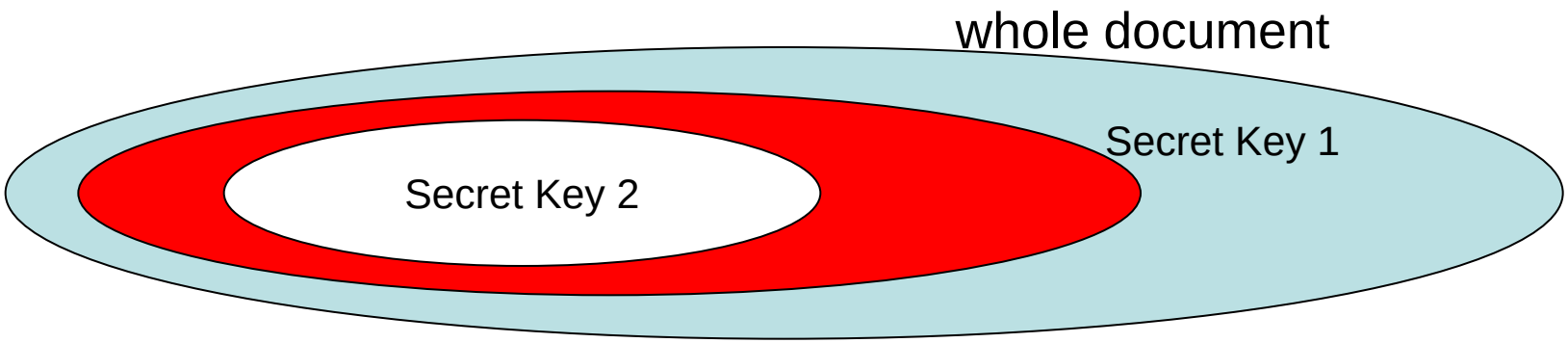


Access Control Scheme by Next Generation Cryptographic Algorithm



New Cryptosystem

- Multivariate Public Key Cryptosystem (MPKC)
- One of Post-Quantum Cryptosystems
- New feature, with an identical Public Key, the range of the decryption defers depending on Secret Keys



Difference between other Systems

	Our Cryptosystem	Conventional system
situation	Access control of the members of organization, depending on the responsibility	Usually designed for Access Control of individuals Control the access depending on the properties of individuals
usage	Dynamically Changes depending on the change of organization, new roles, etc..	Generally Static ,,,, whether the person is US national, over 21, bought the content,,,,
crypto-system	Multi-variate Public Key	ID-base, Pairing, elliptic-curve, ,,

Summary

- Confidential Information and detailed information of operation be protected
- Our proposal assumes medicine and care. But the system is applicable to any situation handling confidential information
- The system is fitted for the "Power to the Edge" organization

Thank you !

- Questions ?