AtlantTIC
Research Center for
Information & Communication Technologies

Secure Genomic Susceptibility Testing based on Lattice Encryption

IEEE International Conference on Acoustics, Speech and Signal Processing

ICASSP 2017, March 5-9, 2017, New Orleans, USA

Juan Ramón Troncoso-Pastoriza
troncoso@gts.uvigo.es
Alberto Pedrouzo-Ulloa
apedrouzo@gts.uvigo.es
Fernando Pérez-González
fperez@gts.uvigo.es

Outline

- Introduction
- Secure Signal Processing
- Private Genomic Susceptibility Testing
- Previous Solutions
- Proposed Scheme
- Security and Performance Evaluation
- Conclusions

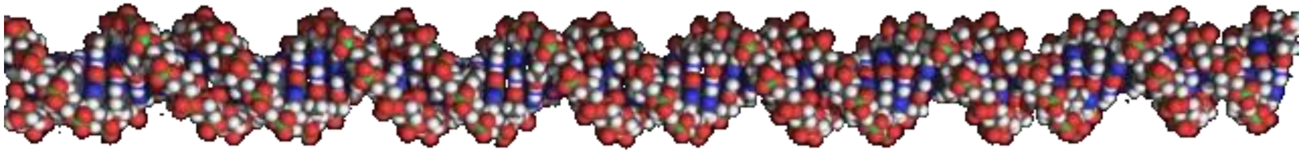
Introduction

Genomic Privacy

Privacy-Preserving Genomic Data Processing

Motivation

- Rapid advances in genomic research and sequencing
- Growing volume of data has to be outsourced
- Inherently sensitive information in DNA (individual and relatives)



Need for privacy-preserving processing!

Privacy-Preserving Genomic Data Processing

Objectives

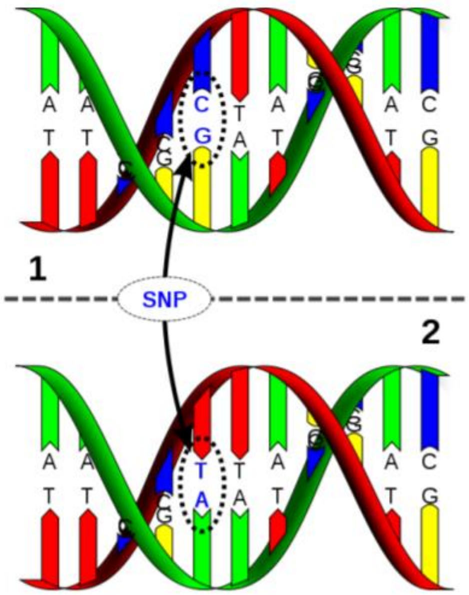
- Personalized health-care (disease susceptibility tests)
- The most common variants in genome are SNPs (Single Nucleotide Polymorphisms)
- SNPs are suitable for running disease susceptibility tests

Privacy-Preserving Genomic Data Processing

Objectives

- Personalized health-care (disease susceptibility tests)
- The most common variants in genome are SNPs (Single Nucleotide Polymorphisms)
- SNPs are suitable for running disease susceptibility tests

The presence and absence of SNPs give information about the susceptibility to a particular disease



Privacy-Preserving Genomic Data Processing

Objectives

- Personalized health-care (disease susceptibility tests)
- The most common variants in genome are SNPs (Single Nucleotide Polymorphisms)
- SNPs are suitable for running disease susceptibility tests

Privacy-Preserving Genomic Data Processing

Objectives

- Personalized health-care (disease susceptibility tests)
- The most common variants in genome are SNPs (Single Nucleotide Polymorphisms)
- SNPs are suitable for running disease susceptibility tests

Contributions

- An efficient protocol for performing encrypted genomic susceptibility tests
- Our solution outperforms previous solutions in both computation, bandwidth and storage

Secure Signal Processing

Privacy tools from SSP

AtlantTIC Research Center for Information & Communication Technologies

Universida de Vigo

Privacy Tools from SSP

Homomorphic Encryption

- Example: Paillier (additive)
  - $E_k(x) = (1 + x \cdot n) \cdot r^n \, mod \, n^2$
  - $E_k(x + y) = E_k(x) \cdot E_k(y) \, mod \, n^2, E_k(x \cdot k) = E_k(x)^k \, mod \, n^2$
- SHE and FHE (both additions and multiplications)

$$(P, +, \cdot) \longrightarrow^{E_k} (C, +, \cdot)$$

- SHE example: Lauter cryptosystem (RLWE based cryptosystem)
- Both homomorphic cyclic convolutions and additions[1]

[1] A. Pedrouzo-Ulloa, J. R. Troncoso-Pastoriza, and F. Pérez-González, "Number Theoretic Transforms for Secure Signal Processing," *in IEEE Transactions on Informations Forensics and Security*, vol.12, no. 5, pp. 1125-1140, May 2017.

Lattice-based SHE Cryptosystem

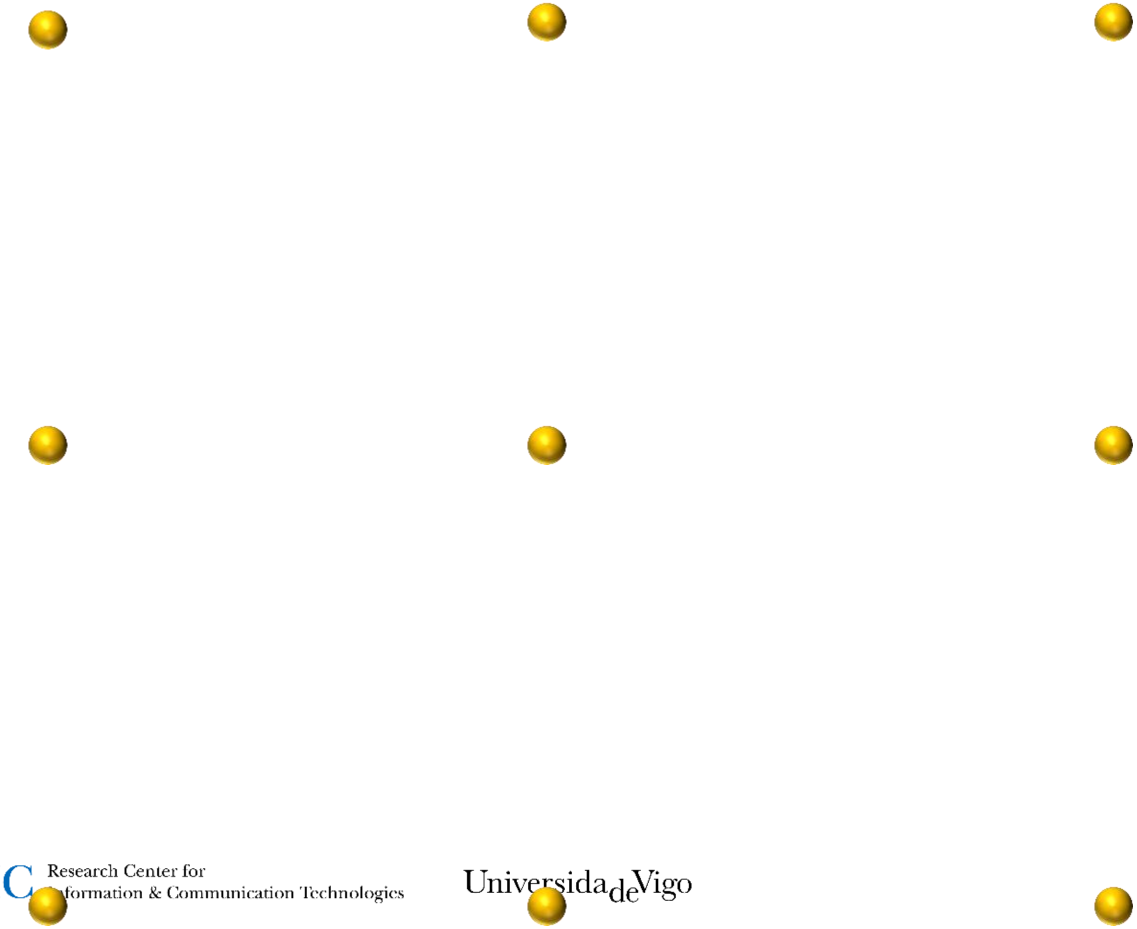
- Somewhat homomorphic cryptosystem

Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations

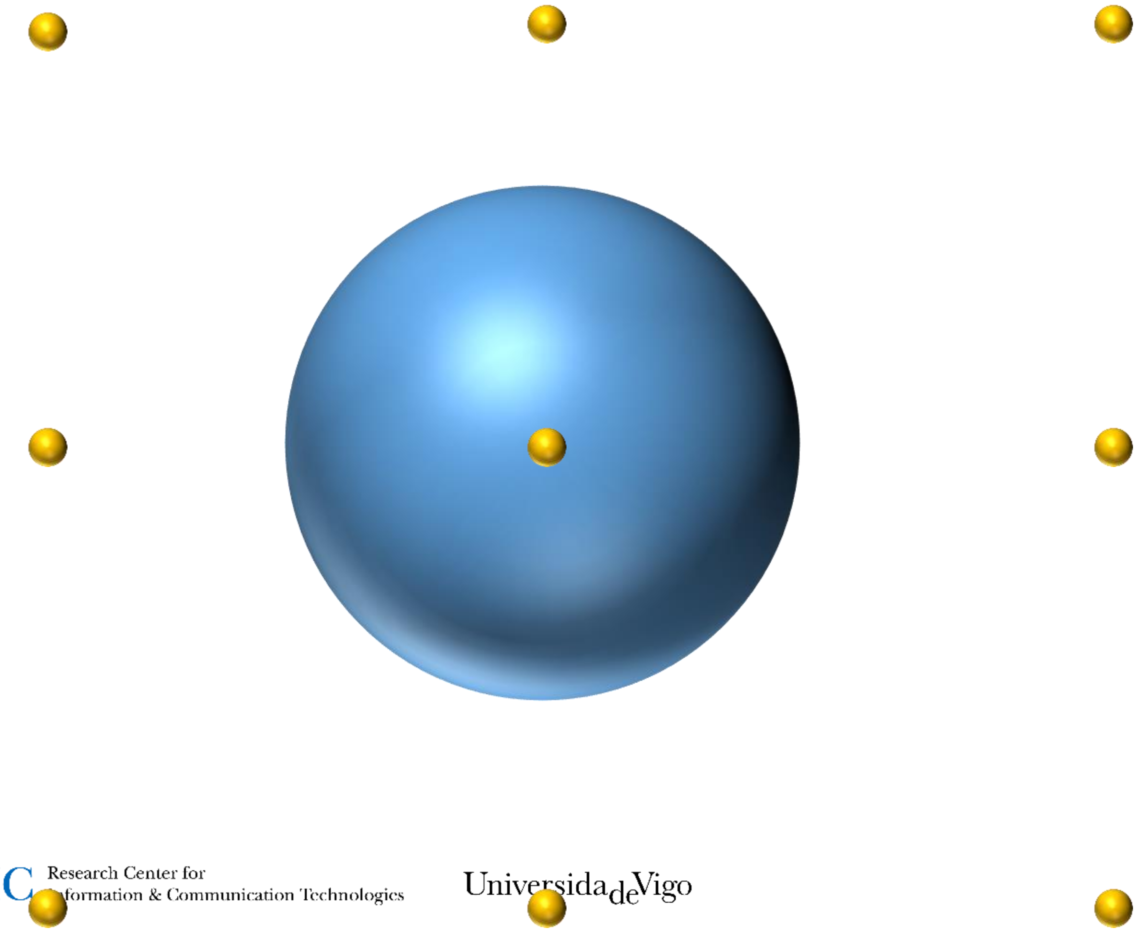
Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations



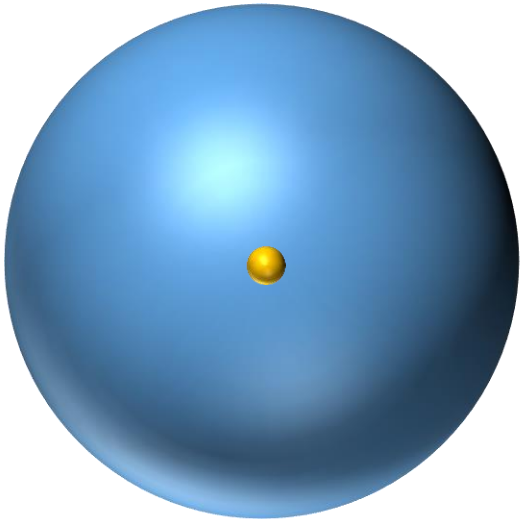
Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations



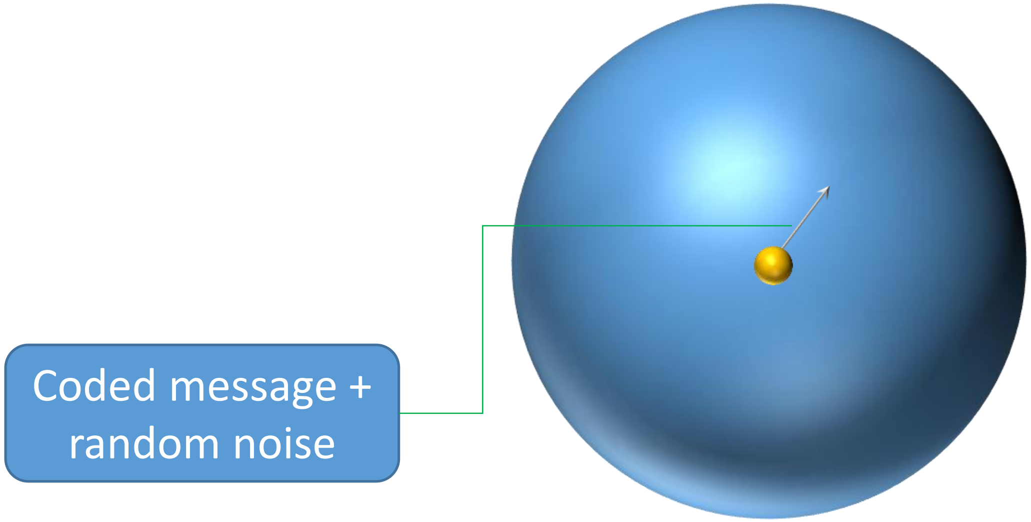
Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations



Lattice-based SHE Cryptosystem

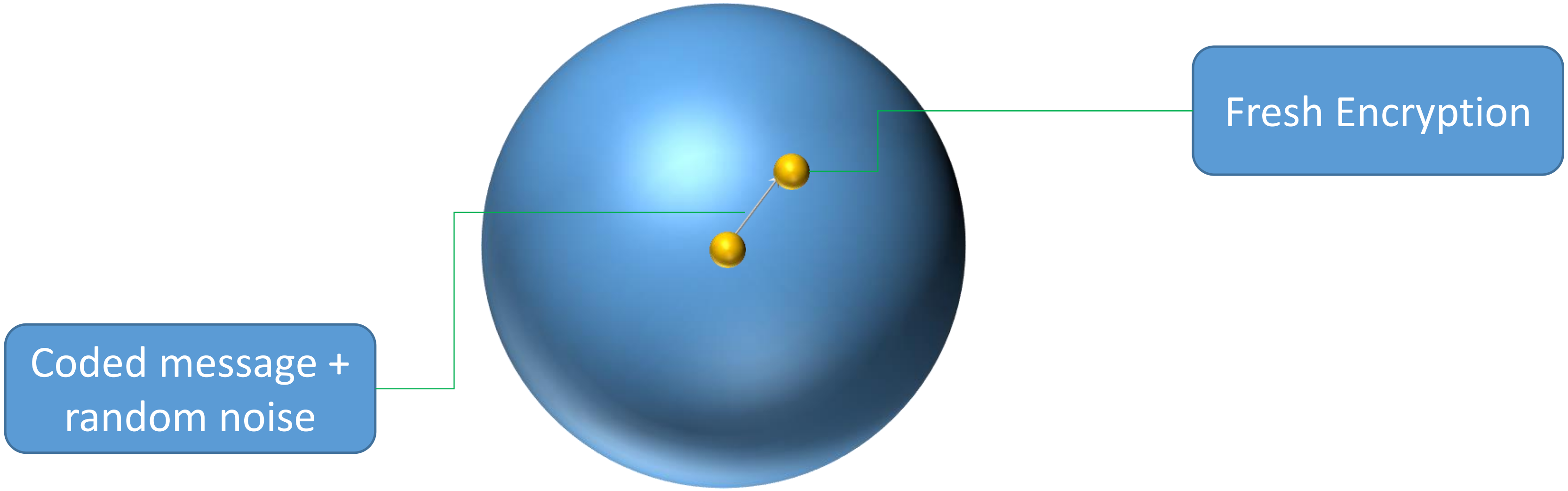
- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations



Coded message + random noise

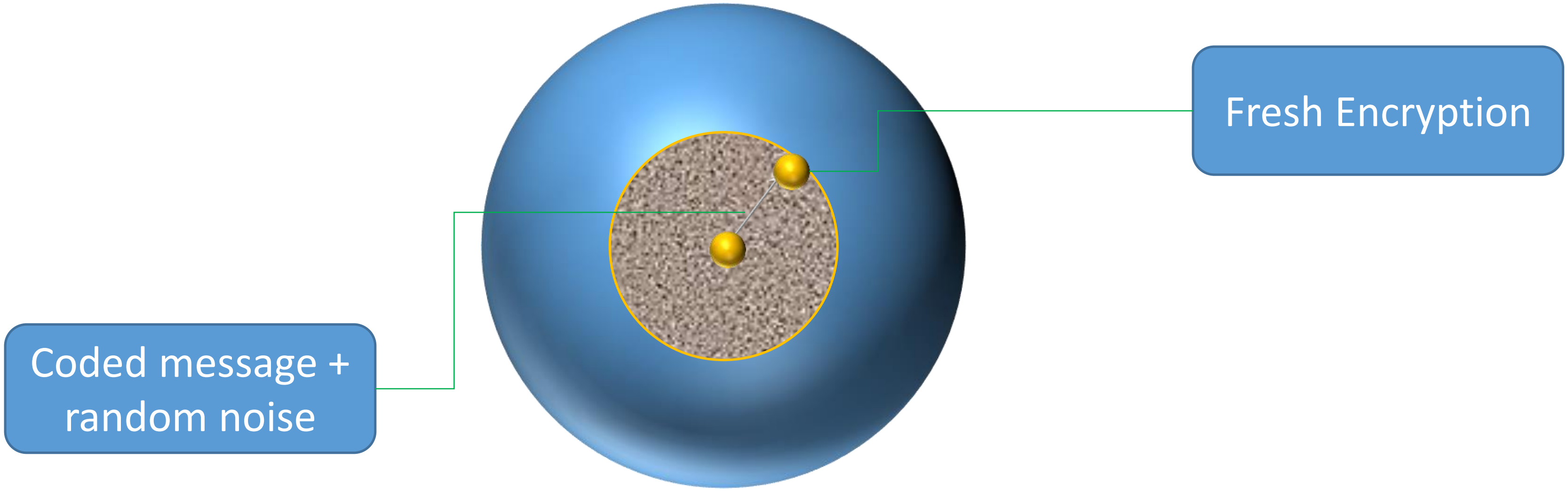
Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations



Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations

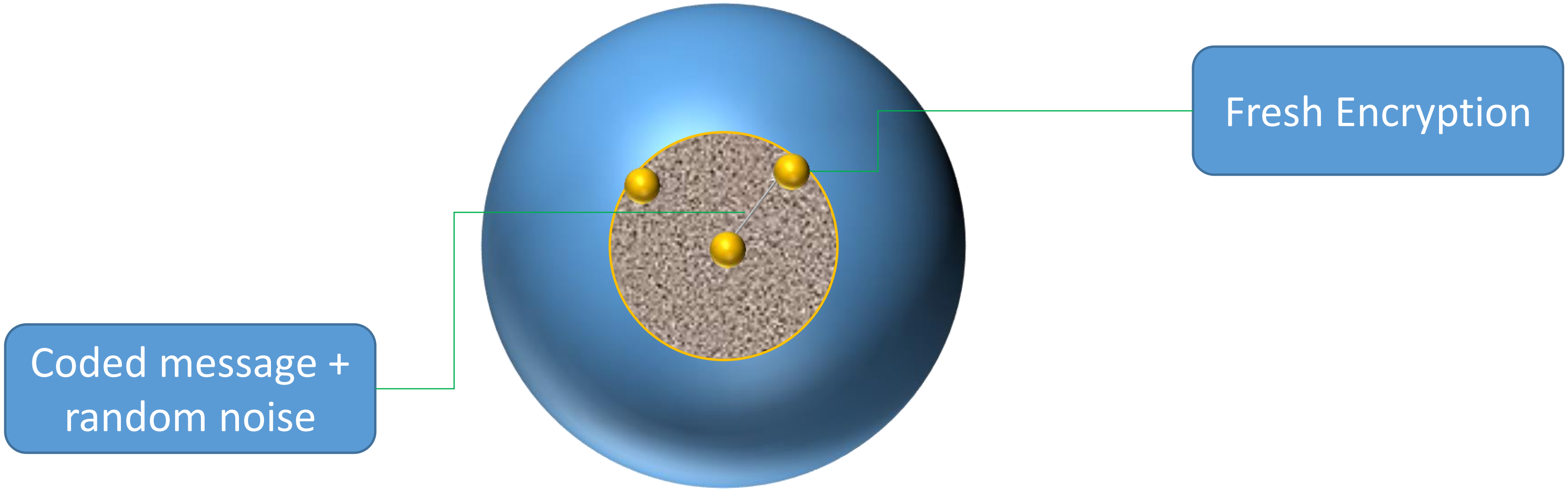


Fresh Encryption

Coded message + random noise

Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations

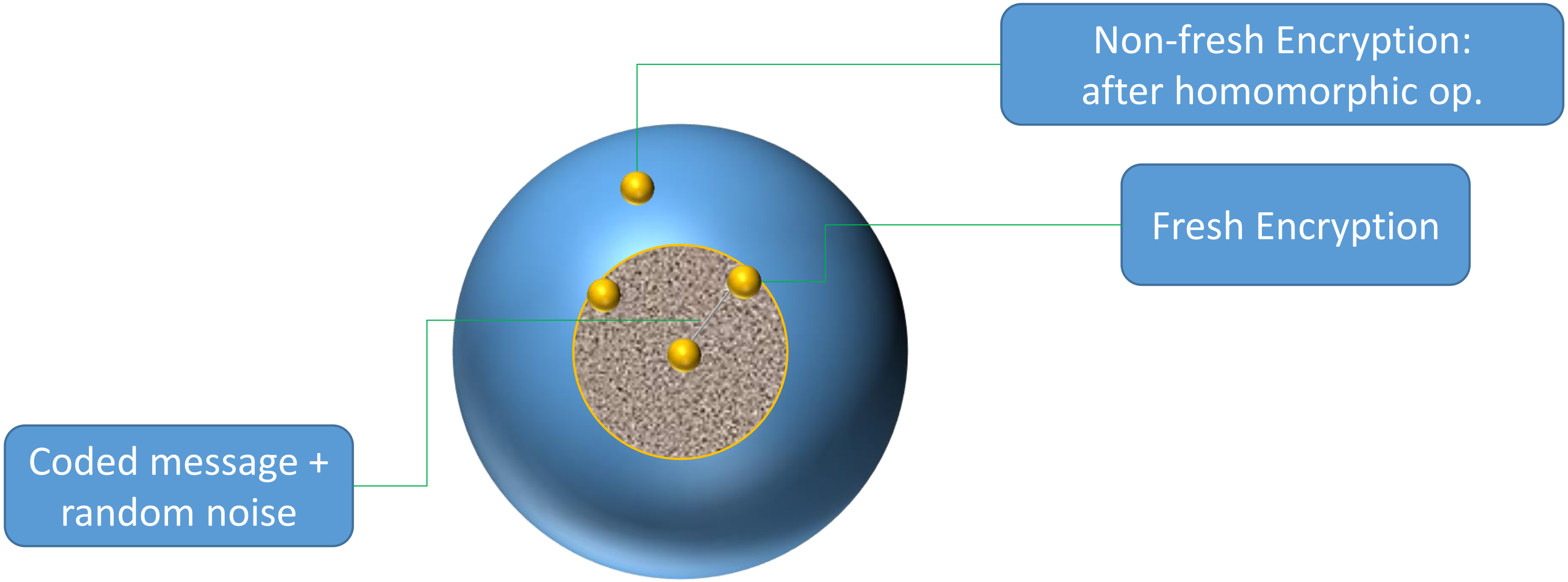


Fresh Encryption

Coded message + random noise

Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations



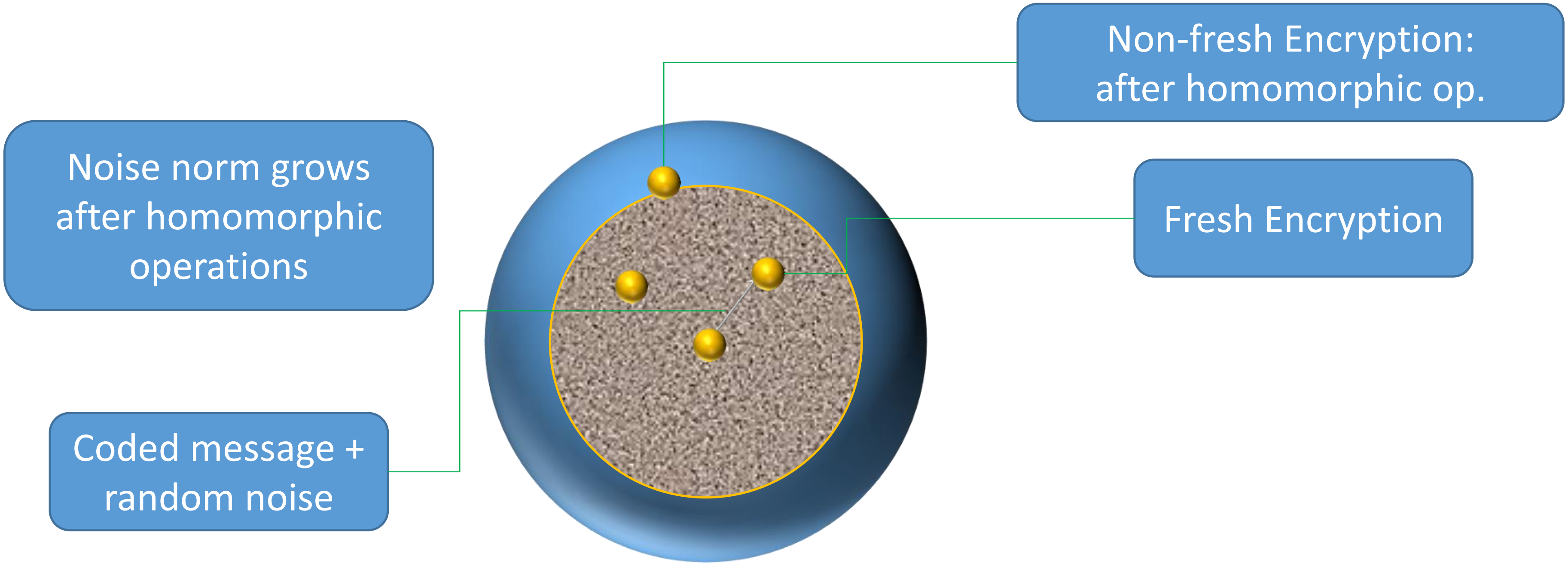
Non-fresh Encryption: after homomorphic op.

Fresh Encryption

Coded message + random noise

Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations



Non-fresh Encryption: after homomorphic op.

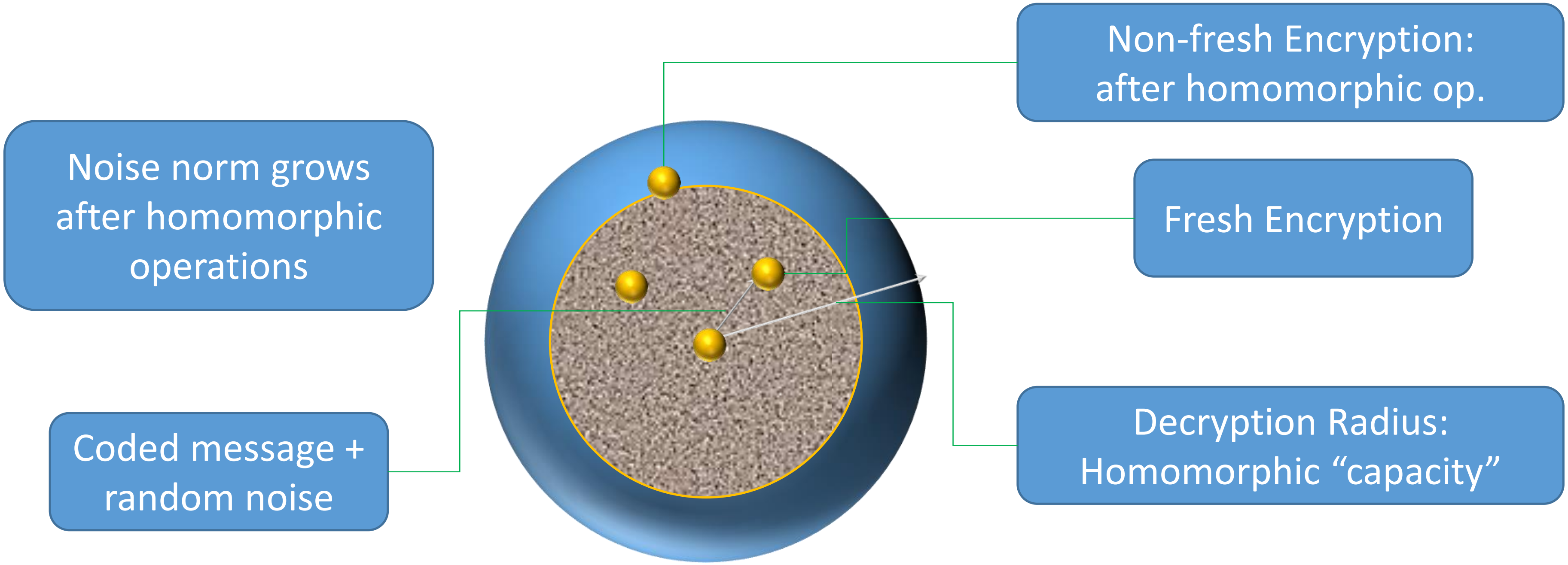
Noise norm grows after homomorphic operations

Fresh Encryption

Coded message + random noise

Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations



Non-fresh Encryption: after homomorphic op.

Noise norm grows after homomorphic operations

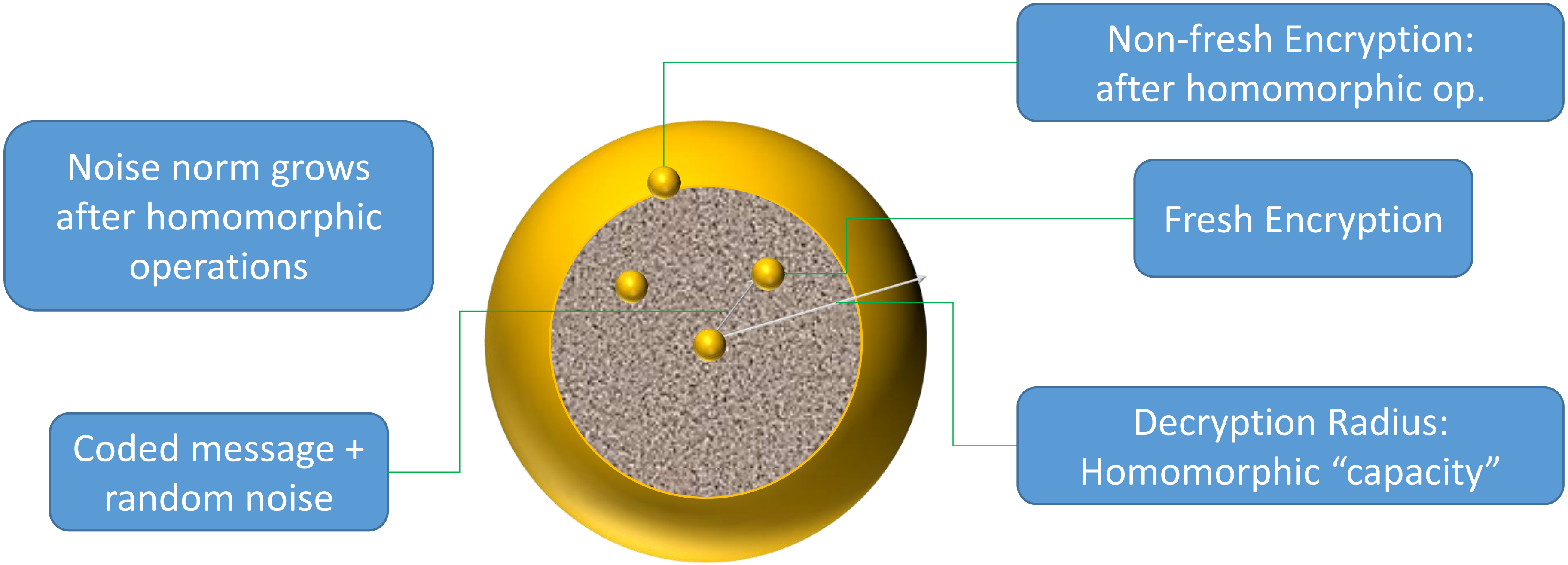
Fresh Encryption

Coded message + random noise

Decryption Radius: Homomorphic “capacity”

Lattice-based SHE Cryptosystem

- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations


Non-fresh Encryption: after homomorphic op.
Noise norm grows after homomorphic operations
Fresh Encryption
Coded message + random noise
Decryption Radius: Homomorphic “capacity”

Lattice-based SHE Cryptosystem

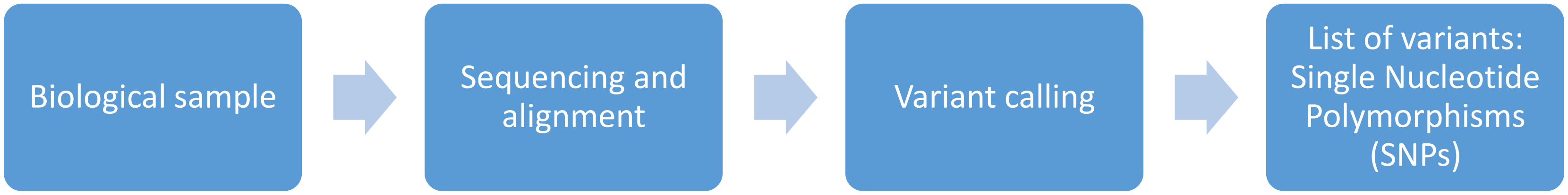
- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations

Lattice-based SHE Cryptosystem

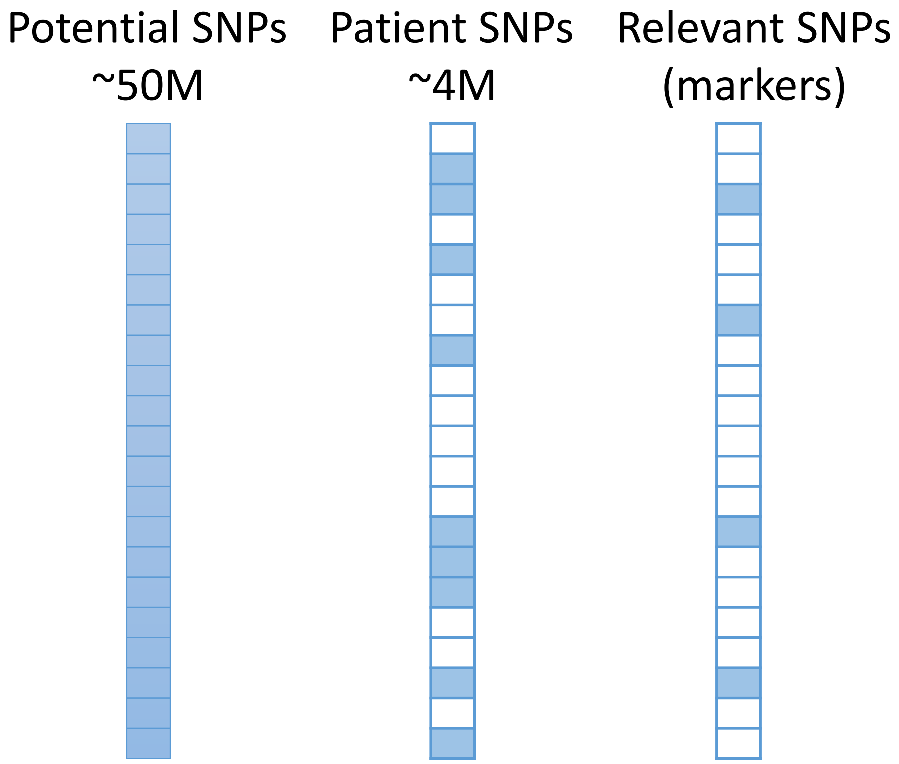
- Somewhat homomorphic cryptosystem
  - Can execute a bounded number of homomorphic operations
  - FHE can get unlimited homomorphic operations
    - FHE is too costly
    - As we know the number of homomorphic operations beforehand, SHE is a perfect candidate for our purposes

Private Genomic Susceptibility Testing

Privacy-preserving genomic susceptibility testing



Biological sample → Sequencing and alignment → Variant calling → List of variants: Single Nucleotide Polymorphisms (SNPs)



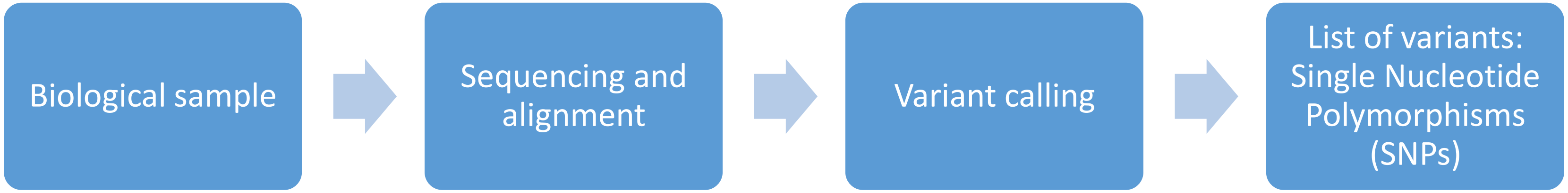
Potential SNPs ~50M

Patient SNPs ~4M

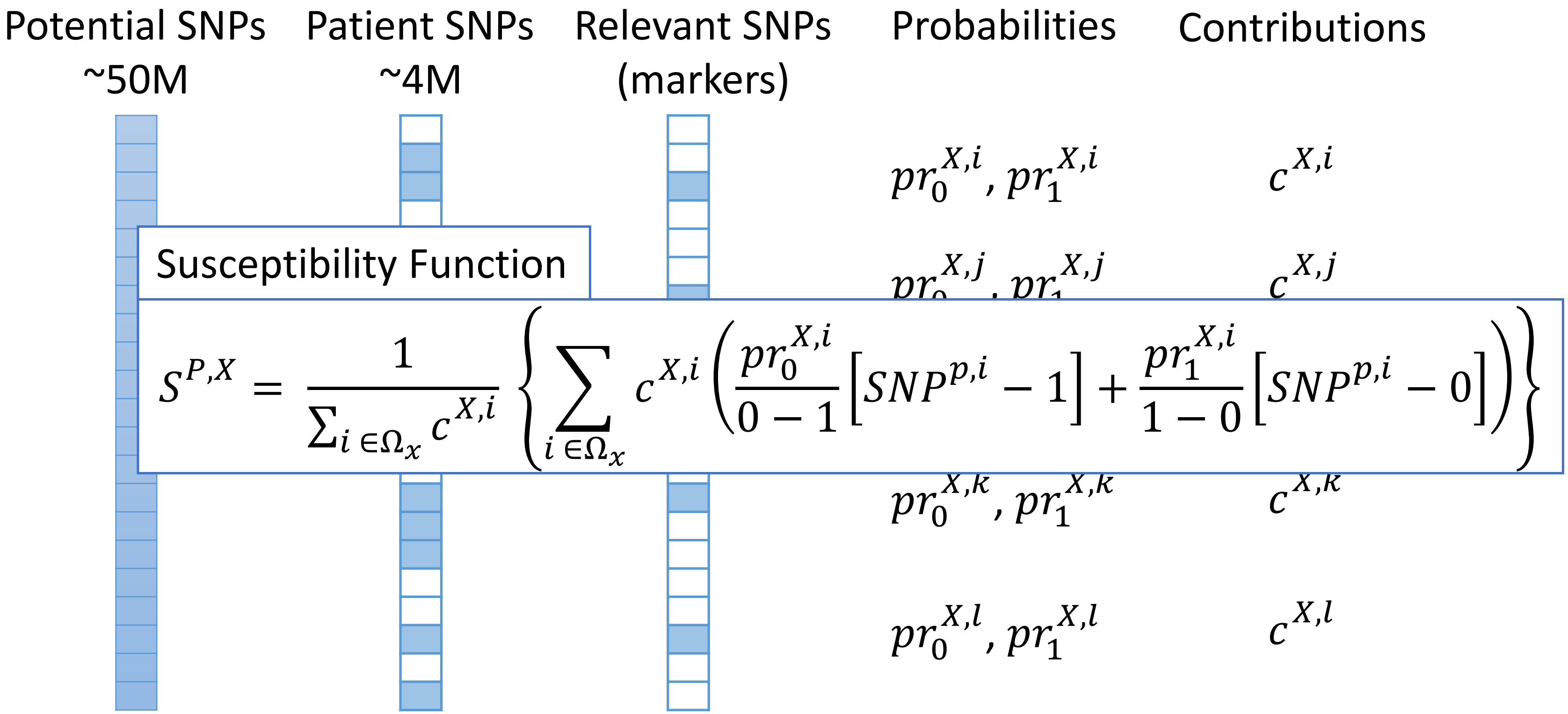
Relevant SNPs (markers)

Probabilities	Contributions
$pr_0^{X,i}, pr_1^{X,i}$	$c^{X,i}$
$pr_0^{X,j}, pr_1^{X,j}$	$c^{X,j}$
$pr_0^{X,k}, pr_1^{X,k}$	$c^{X,k}$
$pr_0^{X,l}, pr_1^{X,l}$	$c^{X,l}$

Privacy-preserving genomic susceptibility testing



Biological sample → Sequencing and alignment → Variant calling → List of variants: Single Nucleotide Polymorphisms (SNPs)



Susceptibility Function

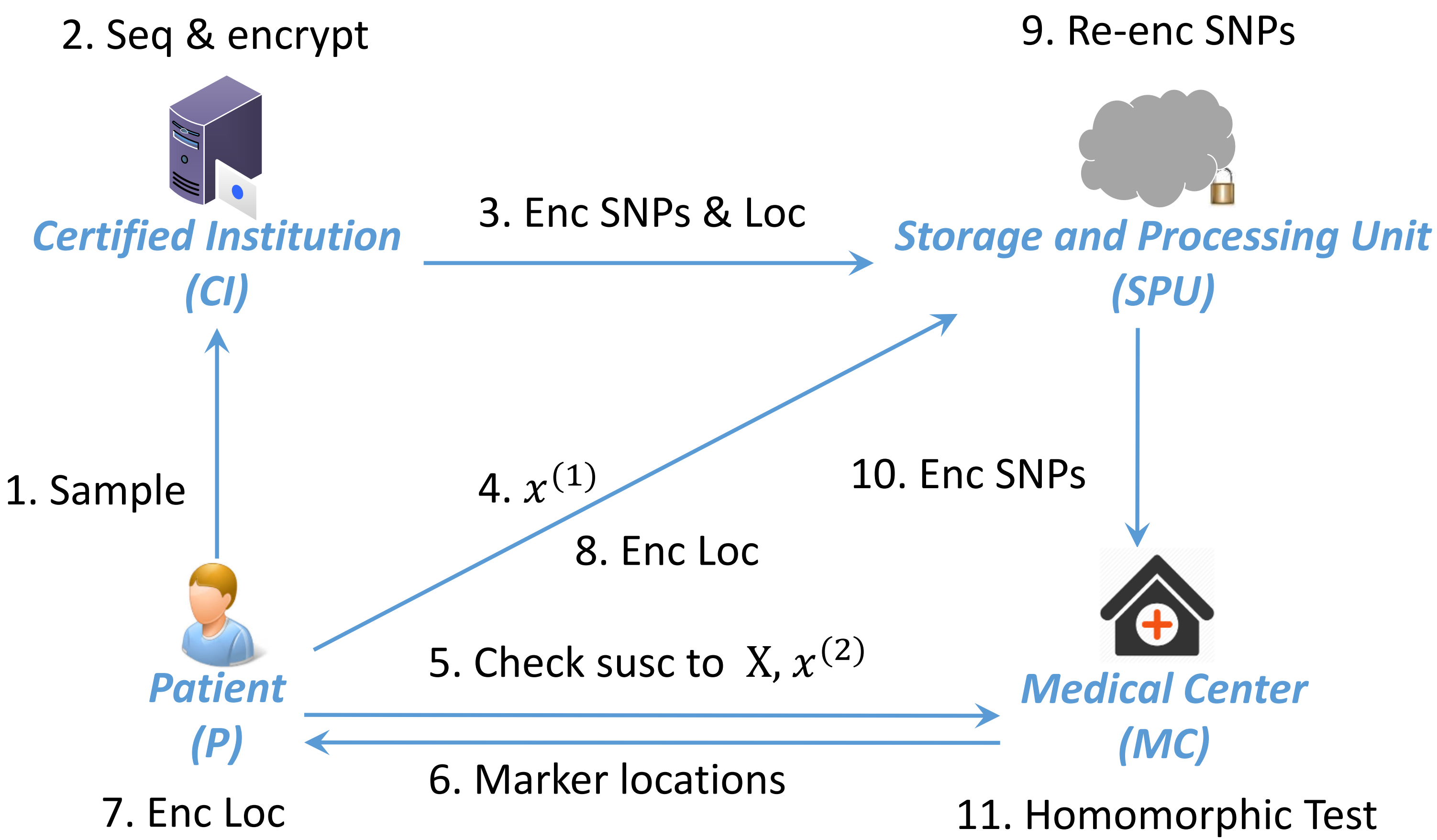
$$S^{P,X} = \frac{1}{\sum_{i \in \Omega_x} c^{X,i}} \left\{ \sum_{i \in \Omega_x} c^{X,i} \left(\frac{pr_0^{X,i}}{0-1} \left[SNP^{p,i} - 1 \right] + \frac{pr_1^{X,i}}{1-0} \left[SNP^{p,i} - 0 \right] \right) \right\}$$

Previous Schemes

Ayday et al. [2]

[2] E. Ayday, J. L. Raisaro, and J. P. Hubaux, "Privacy-Enhancing Technologies for Medical Tests Using Genomic Data," *in 20th Annual Network & Distributed System Security Symposium NDSS*, San Diego, CA, USA, Feb. 2013.

Privacy-preserving genomic susceptibility testing



2. Seq & encrypt

Certified Institution (CI)

3. Enc SNPs & Loc

9. Re-enc SNPs

Storage and Processing Unit (SPU)

1. Sample

4. $x^{(1)}$

8. Enc Loc

10. Enc SNPs

Patient (P)

5. Check susc to X, $x^{(2)}$

6. Marker locations

Medical Center (MC)

7. Enc Loc

11. Homomorphic Test

Privacy-preserving genomic susceptibility testing

Susceptibility Function

$$S^{P,X} = \frac{1}{\sum_{i \in \Omega_x} c^{X,i}} \left\{ \sum_{i \in \Omega_x} c^{X,i} \left(\frac{pr_0^{X,i}}{0-1} \left[SNP^{p,i} - 1 \right] + \frac{pr_1^{X,i}}{1-0} \left[SNP^{p,i} - 0 \right] \right) \right\}$$

Privacy-preserving genomic susceptibility testing

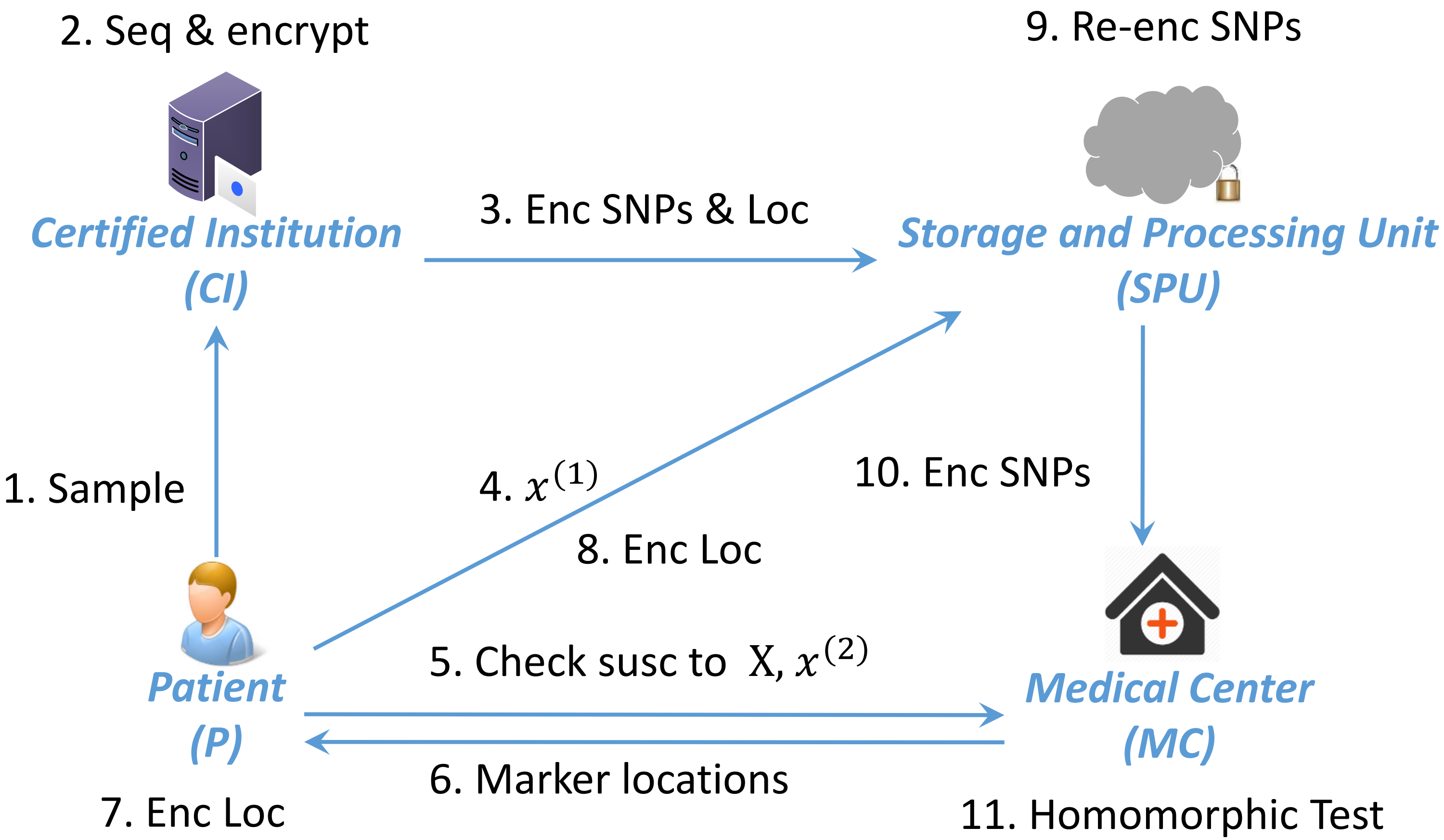
Susceptibility Function

$$S^{P,X} = \frac{1}{\sum_{i\in\Omega_x} c^{X,i}} \left\{ \sum_{i\in\Omega_x} c^{X,i} \left(\frac{pr_0^{X,i}}{0-1}\left[SNP^{p,i}-1\right] + \frac{pr_1^{X,i}}{1-0}\left[SNP^{p,i}-0\right] \right) \right\}$$

Paillier-encrypted Susceptibility

$$S_E^{P,X} = \prod_{i\in\Omega_x} \left(\left[SNP_E^{p,i}\cdot(-1)_E\right]^{\frac{-c^{X,i}\cdot pr_0^{X,i}}{\sum_{i\in\Omega_x} c^{X,i}}} \cdot \left[SNP_E^{p,i}\right]^{\frac{c^{X,i}\cdot pr_1^{X,i}}{\sum_{i\in\Omega_x} c^{X,i}}} \right)$$

Privacy-preserving genomic susceptibility testing



2. Seq & encrypt

9. Re-enc SNPs

Certified Institution (CI)

3. Enc SNPs & Loc

Storage and Processing Unit (SPU)

1. Sample

4. $x^{(1)}$

10. Enc SNPs

8. Enc Loc

Patient (P)

5. Check susc to X, $x^{(2)}$

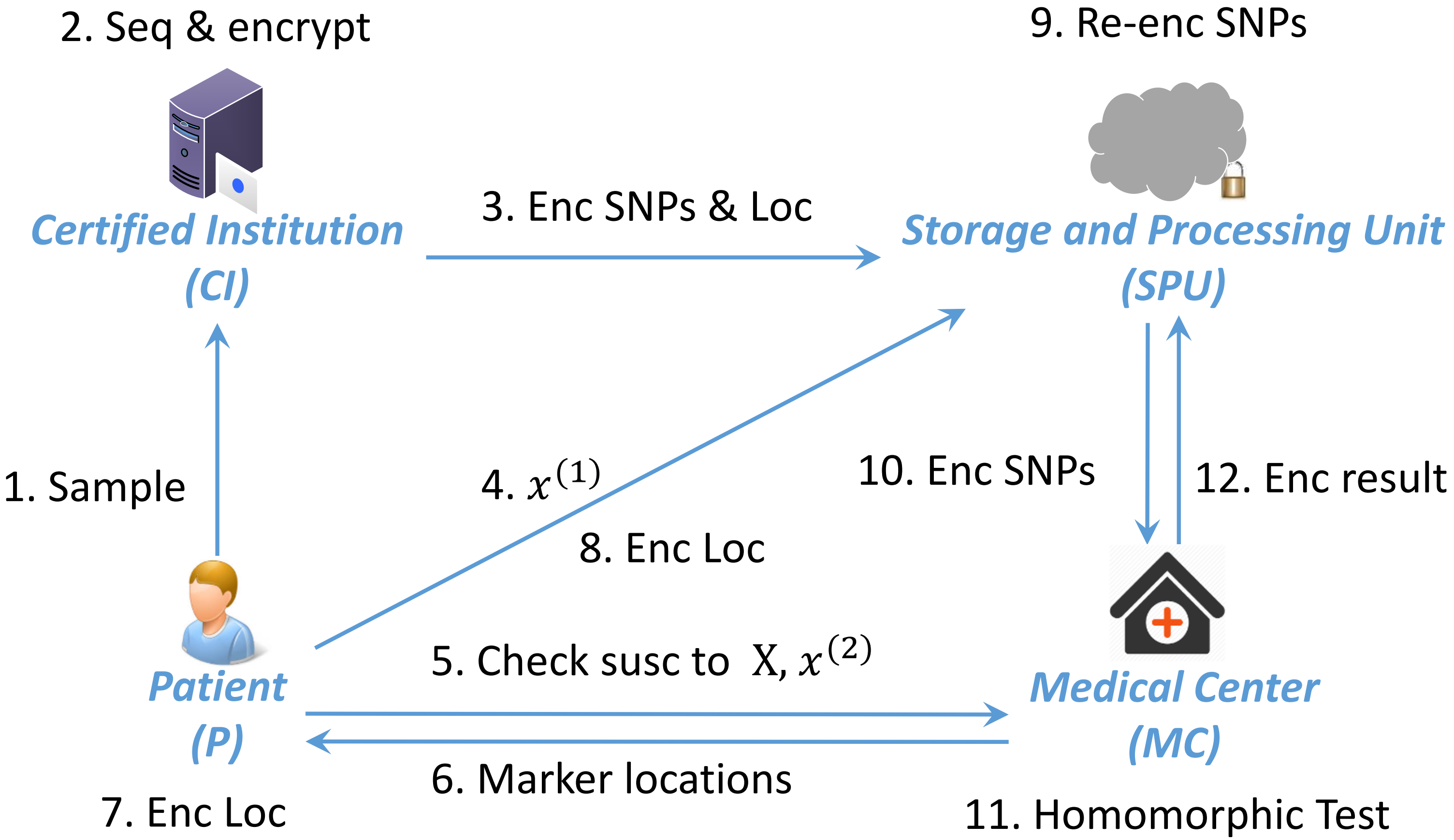
Medical Center (MC)

6. Marker locations

7. Enc Loc

11. Homomorphic Test

Privacy-preserving genomic susceptibility testing



2. Seq & encrypt

9. Re-enc SNPs

Certified Institution (CI)

3. Enc SNPs & Loc

Storage and Processing Unit (SPU)

1. Sample

4. $x^{(1)}$

8. Enc Loc

10. Enc SNPs

12. Enc result

Patient (P)

5. Check susc to X, $x^{(2)}$

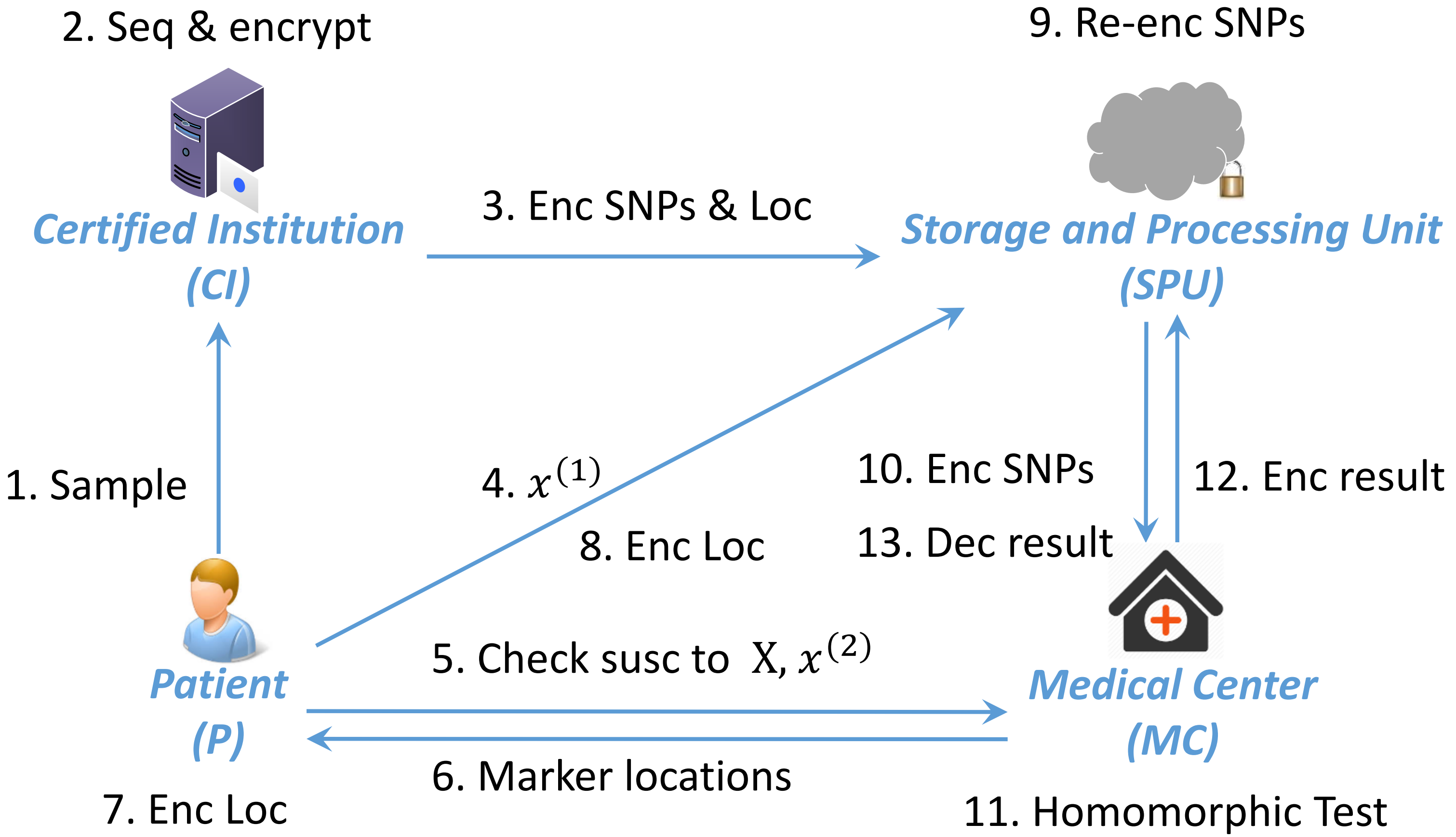
Medical Center (MC)

6. Marker locations

7. Enc Loc

11. Homomorphic Test

Privacy-preserving genomic susceptibility testing



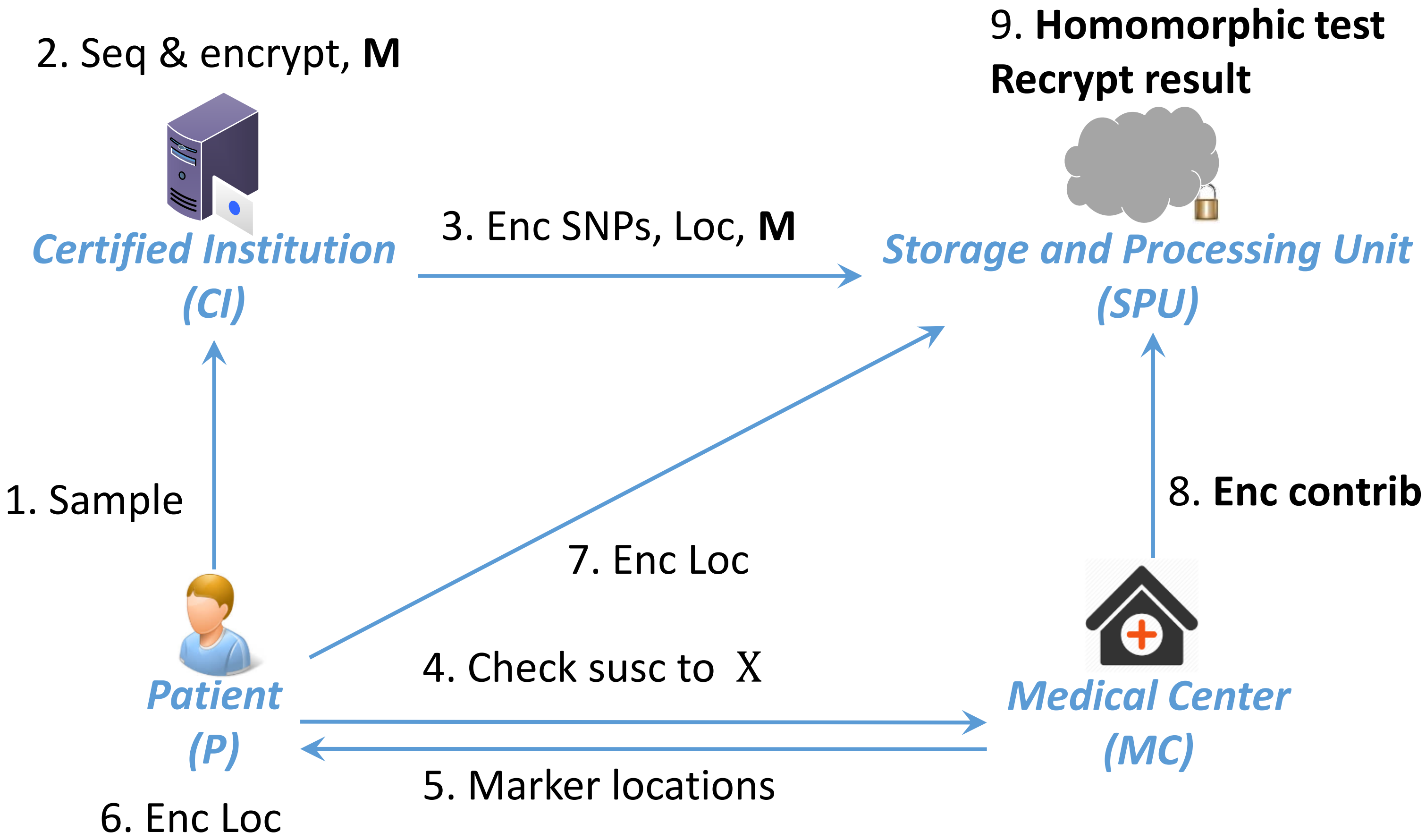
Previous Schemes

Namazi et al. [3]

[3] M. Namazi, J. R. Troncoso-Pastoriza, and F. Pérez-González, “Dynamic Privacy-Preserving Genomic Susceptibility Testing,” *in Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*. 2016, IH&MMSec`16, pp. 45-50, ACM.

Privacy-preserving genomic susceptibility testing

- Modified scheme with lattice-based encryptions [NTP16]


2. Seq & encrypt, **M**

Certified Institution (CI)

3. Enc SNPs, Loc, **M**

9. **Homomorphic test**
Recrypt result

Storage and Processing Unit (SPU)

1. Sample

7. Enc Loc

8. **Enc contrib**

Patient (P)

4. Check susc to X

Medical Center (MC)

5. Marker locations

6. Enc Loc

Privacy-preserving genomic susceptibility testing

- Modified scheme with lattice-based encryptions [NTP16]

Susceptibility Function

$$S^{P,X} = \frac{1}{\sum_{i \in \Omega_x} c^{X,i}} \left\{ \sum_{i \in \Omega_x} c^{X,i} \left(\frac{pr_0^{X,i}}{0-1} \left[SNP^{p,i} - 1 \right] + \frac{pr_1^{X,i}}{1-0} \left[SNP^{p,i} - 0 \right] \right) \right\}$$

Privacy-preserving genomic susceptibility testing

- Modified scheme with lattice-based encryptions [NTP16]

Susceptibility Function

$$S^{P,X} = \frac{1}{\sum_{i \in \Omega_x} c^{X,i}} \left\{ \sum_{i \in \Omega_x} c^{X,i} \left(\frac{pr_0^{X,i}}{0-1} \left[SNP^{p,i} - 1 \right] + \frac{pr_1^{X,i}}{1-0} \left[SNP^{p,i} - 0 \right] \right) \right\}$$

Lauter-encrypted Susceptibility

$$S_E^{P,X} = \sum_{i \in \Omega_x} \left(\left[\frac{-c^{X,i} pr_0^{X,i}}{\sum_{i \in \Omega_x} c^{X,i}} \right]_E \cdot \left[SNP_E^{p,i} - 1 \right] + \left[\frac{c^{X,i} pr_1^{X,i}}{\sum_{i \in \Omega_x} c^{X,i}} \right]_E \cdot \left[SNP_E^{p,i} \right] \right)$$

Privacy-preserving genomic susceptibility testing

- Modified scheme with lattice-based encryptions [NTP16]

Susceptibility Function

$$S^{P,X} = \frac{1}{\sum_{i\,\in\Omega_x} c^{X,i}} \left\{ \sum_{i\,\in\Omega_x} c^{X,i} \left(\frac{pr_0^{X,i}}{0-1} \left[SNP^{p,i} - 1 \right] + \frac{pr_1^{X,i}}{1-0} \left[SNP^{p,i} - 0 \right] \right) \right\}$$

Lauter-encrypted Susceptibility

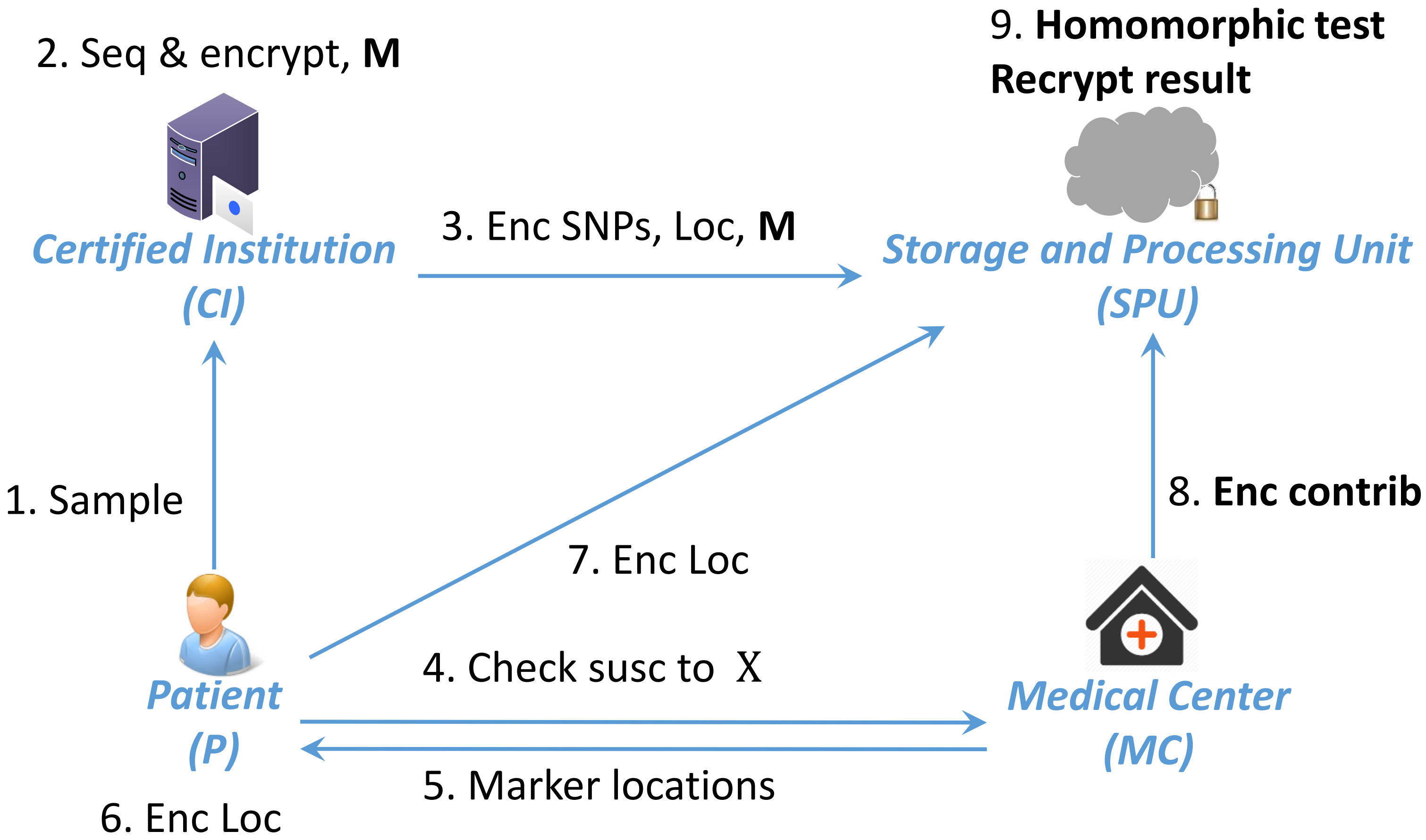
$$S_E^{P,X} = \sum_{i\,\in\Omega_x} \left(\left[\frac{-c^{X,i} pr_0^{X,i}}{\sum_{i\,\in\Omega_x} c^{X,i}} \right]_E \cdot \left[SNP_E^{p,i} - 1 \right] + \left[\frac{c^{X,i} pr_1^{X,i}}{\sum_{i\,\in\Omega_x} c^{X,i}} \right]_E \cdot \left[SNP_E^{p,i} \right] \right)$$

Paillier-encrypted Susceptibility

$$S_E^{P,X} = \prod_{i\,\in\Omega_x} \left(\left[SNP_E^{p,i} \cdot (-1)_E \right]^{\frac{-c^{X,i} \cdot pr_0^{X,i}}{\sum_{i\,\in\Omega_x} c^{X,i}}} \cdot \left[SNP_E^{p,i} \right]^{\frac{c^{X,i} \cdot pr_1^{X,i}}{\sum_{i\,\in\Omega_x} c^{X,i}}} \right)$$

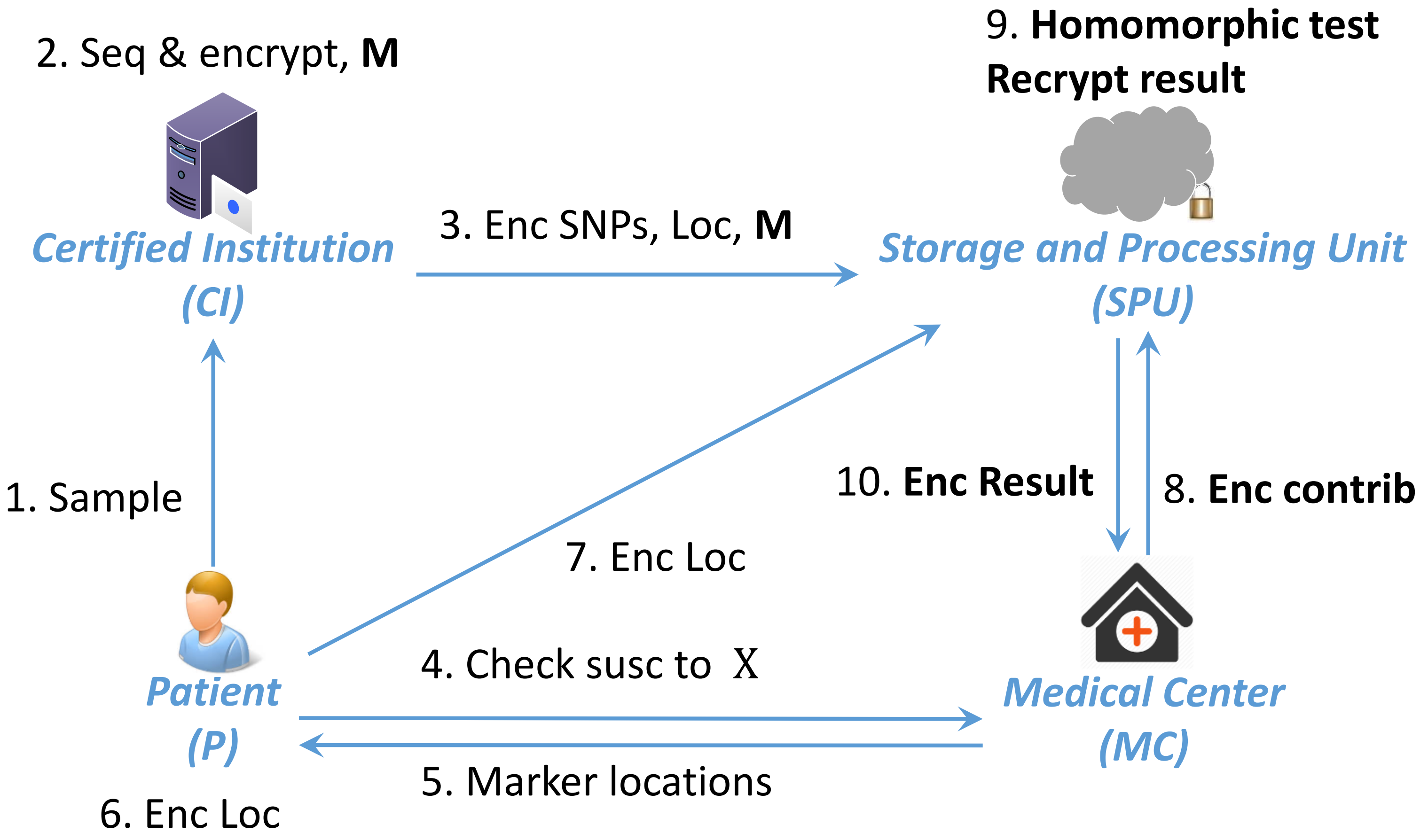
Privacy-preserving genomic susceptibility testing

- Modified scheme with lattice-based encryptions [NTP16]



Privacy-preserving genomic susceptibility testing

- Modified scheme with lattice-based encryptions [NTP16]



2. Seq & encrypt, **M**

Certified Institution (CI)

9. **Homomorphic test Recrypt result**

Storage and Processing Unit (SPU)

3. Enc SNPs, Loc, **M**

1. Sample

7. Enc Loc

10. **Enc Result**

8. **Enc contrib**

Patient (P)

Medical Center (MC)

4. Check susc to X

5. Marker locations

6. Enc Loc

Privacy-preserving genomic susceptibility testing

- Complexity
  - 4M SNPs, 10-marker test
  - Paillier: 2048-bit modulus, Lauter: 4096-dim. lattice

Ayday et al.	CI	SPU		MC	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4,1 GB	10.2 kB	1.02 kB	1.02 kB	

Namazi et al.	CI	SPU		MC	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.45 ms	2.17 ms	2.32 ms	9.1 ms	0.96 ms
Size	262,1 GB		65,5 kB	1,31 MB	

Privacy-preserving genomic susceptibility testing

- Complexity
  - 4M SNPs, 10-marker test
  - Paillier: 2048-bit modulus, Lauter: 4096-dim. lattice

Ayday et al.	CI	SPU		MC	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4,1 GB	10.2 kB	1.02 kB	1.02 kB	

Namazi et al.	CI	SPU		MC	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.45 ms	2.17 ms	2.32 ms	9.1 ms	0.96 ms
Size	262,1 GB		65,5 kB	1,31 MB	

Privacy-preserving genomic susceptibility testing

- Complexity
  - 4M SNPs, 10-marker test
  - Paillier: 2048-bit modulus, Lauter: 4096-dim. lattice

Ayday et al.	CI	SPU		MC	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4,1 GB	10.2 kB	1.02 kB	1.02 kB	

Namazi et al.	CI	SPU		MC	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.45 ms	2.17 ms	2.32 ms	9.1 ms	0.96 ms
Size	262,1 GB		65,5 kB	1,31 MB	

Privacy-preserving genomic susceptibility testing

- Complexity
  - 4M SNPs, 10-marker test
  - Paillier: 2048-bit modulus, Lauter: 4096-dim. lattice

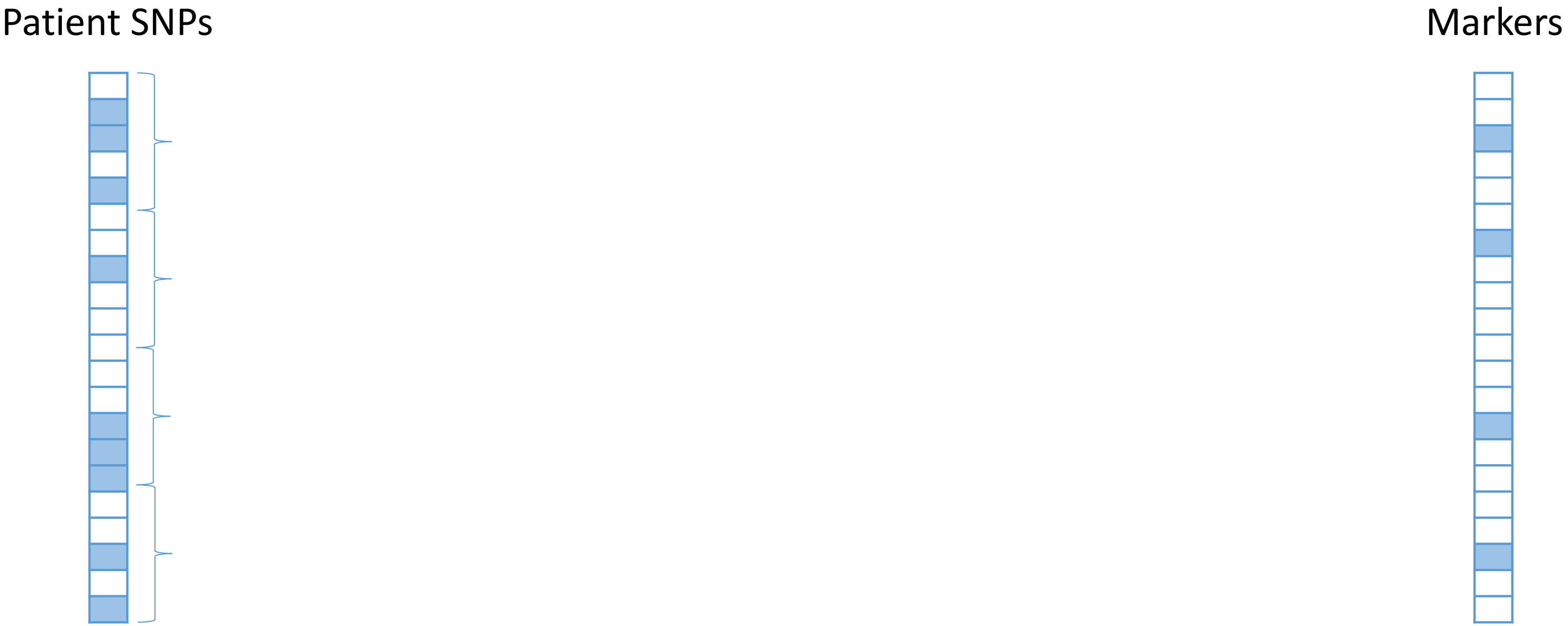
Ayday et al.	**CI**	**SPU**		**MC**	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4,1 GB	10.2 kB	1.02 kB	1.02 kB	

Namazi et al.	**CI**	**SPU**		**MC**	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.45 ms	2.17 ms	2.32 ms	9.1 ms	0.96 ms
Size	262,1 GB		65,5 kB	1,31 MB	

Proposed Scheme

Privacy-preserving genomic susceptibility testing

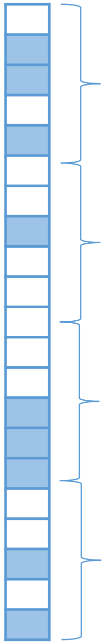
- One step further: packing
  - Reduce cipher expansion



Privacy-preserving genomic susceptibility testing

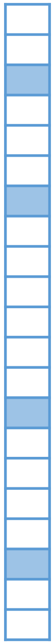
- One step further: packing
  - Reduce cipher expansion

Patient SNPs



$$SN = \left(\sum_{i \in P} SNP^{p,i} \cdot z^{i} \right)$$

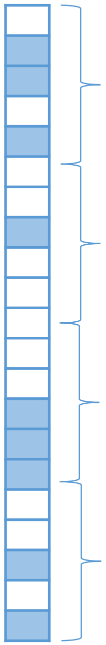
Markers



Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion

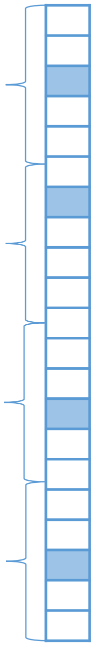
Patient SNPs



$$SN = \left(\sum_{i \in P} SNP^{p,i} \cdot z^{i} \right)$$

$$\beta_b = \left[\sum_{i \in \Omega_x} \frac{(-1)^{1-b} c^{X,i} pr_b^{X,i}}{\sum_{i \in \Omega_x} c^{X,i}} \cdot z^{i} \right]$$

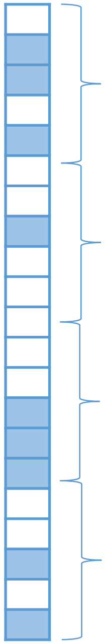
Markers



Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available

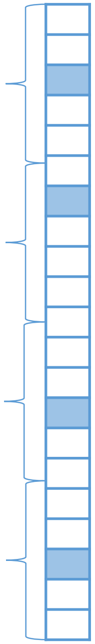
Patient SNPs



$$SN = \left(\sum_{i\in P} SNP^{p,i}\cdot z^{i}\right)$$

$$\beta_b = \left[\sum_{i\in\Omega_x} \frac{(-1)^{1-b}\, c^{X,i}\, pr_b^{X,i}}{\sum_{i\,\in\Omega_x} c^{X,i}}\cdot z^{i}\right]$$

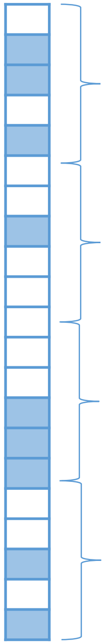
Markers



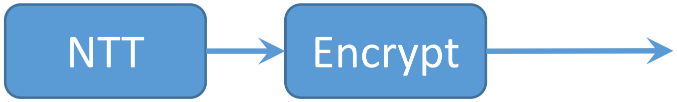
Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available

Patient SNPs

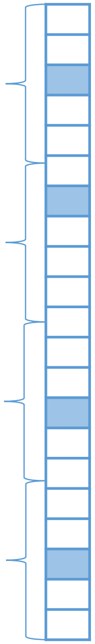


$$SN = \left(\sum_{i\in P} SNP^{p,i}\cdot z^{i}\right)$$



Markers

$$\beta_b = \left[\sum_{i\in\Omega_x} \frac{(-1)^{1-b} c^{X,i} pr_b^{X,i}}{\sum_{i\,\in\Omega_x} c^{X,i}}\cdot z^{i}\right]$$

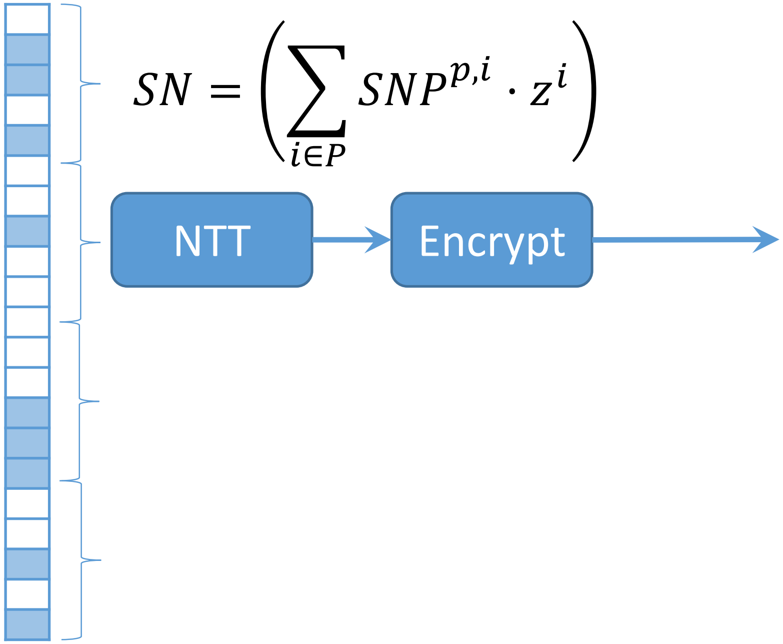


Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available

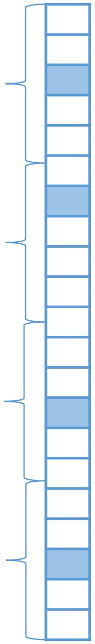
$$NTT[\boldsymbol{x}]_k = \sum_{i\in[0,N)} x_i \alpha^{i\cdot k}$$

Patient SNPs



$$SN = \left(\sum_{i\in P} SNP^{p,i} \cdot z^i\right)$$

Markers



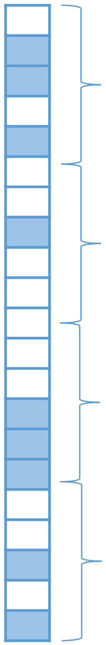
$$\beta_b = \left[\sum_{i\in\Omega_x} \frac{(-1)^{1-b} c^{X,i} pr_b^{X,i}}{\sum_{i\,\in\Omega_x} c^{X,i}} \cdot z^i\right]$$

Privacy-preserving genomic susceptibility testing

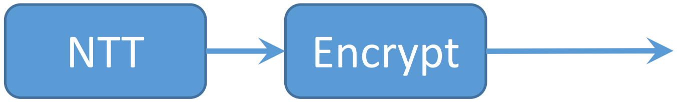
- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available

$$NTT[\boldsymbol{x}]_k = \sum_{i\in[0,N)} x_i \alpha^{i\cdot k}$$

Patient SNPs

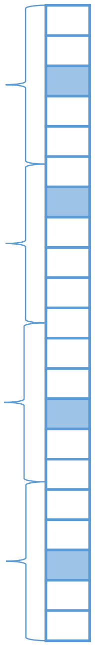


$$SN_E = \left(NTT\left[\sum_{i\in P} SNP^{p,i}\cdot z^i\right]\right)_E$$



$$\beta_b = \left[\sum_{i\in\Omega_x} \frac{(-1)^{1-b} c^{X,i} pr_b^{X,i}}{\sum_{i\in\Omega_x} c^{X,i}}\cdot z^i\right]$$

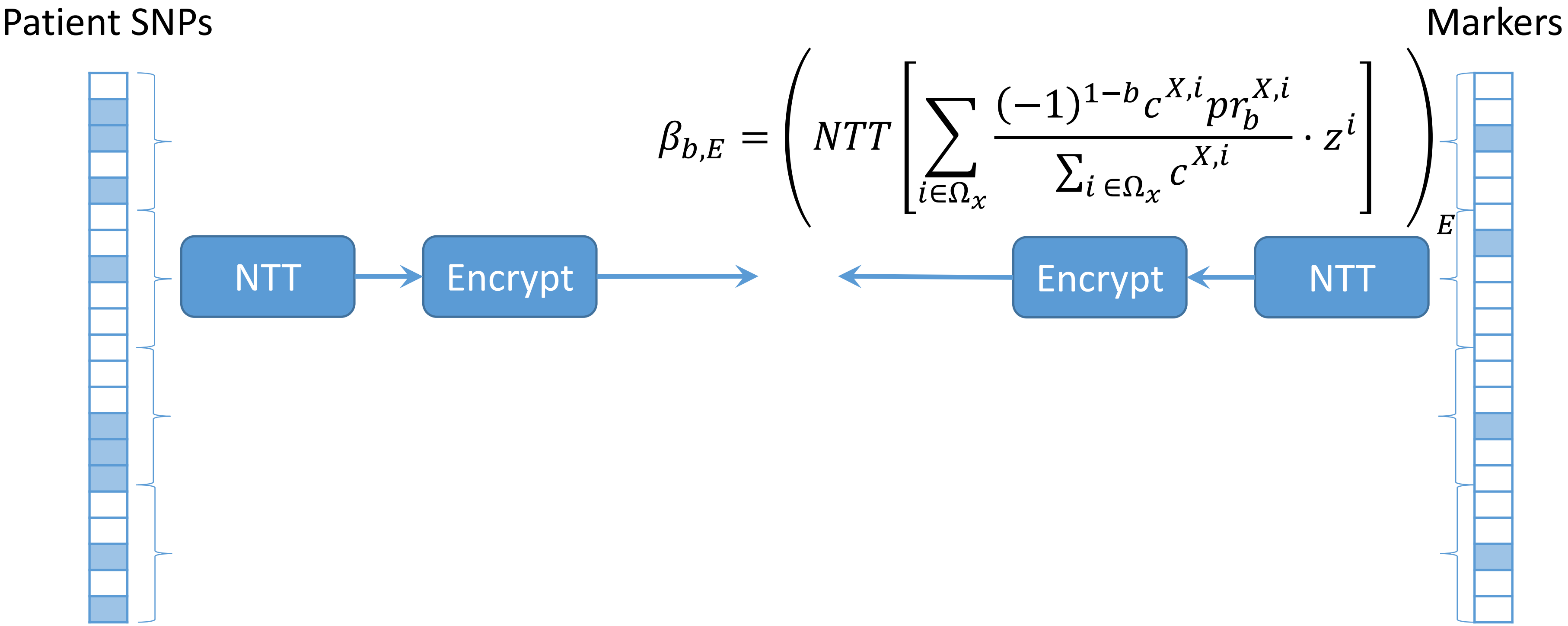
Markers



Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available

$$NTT[\boldsymbol{x}]_k = \sum_{i\in[0,N)} x_i \alpha^{i\cdot k}$$

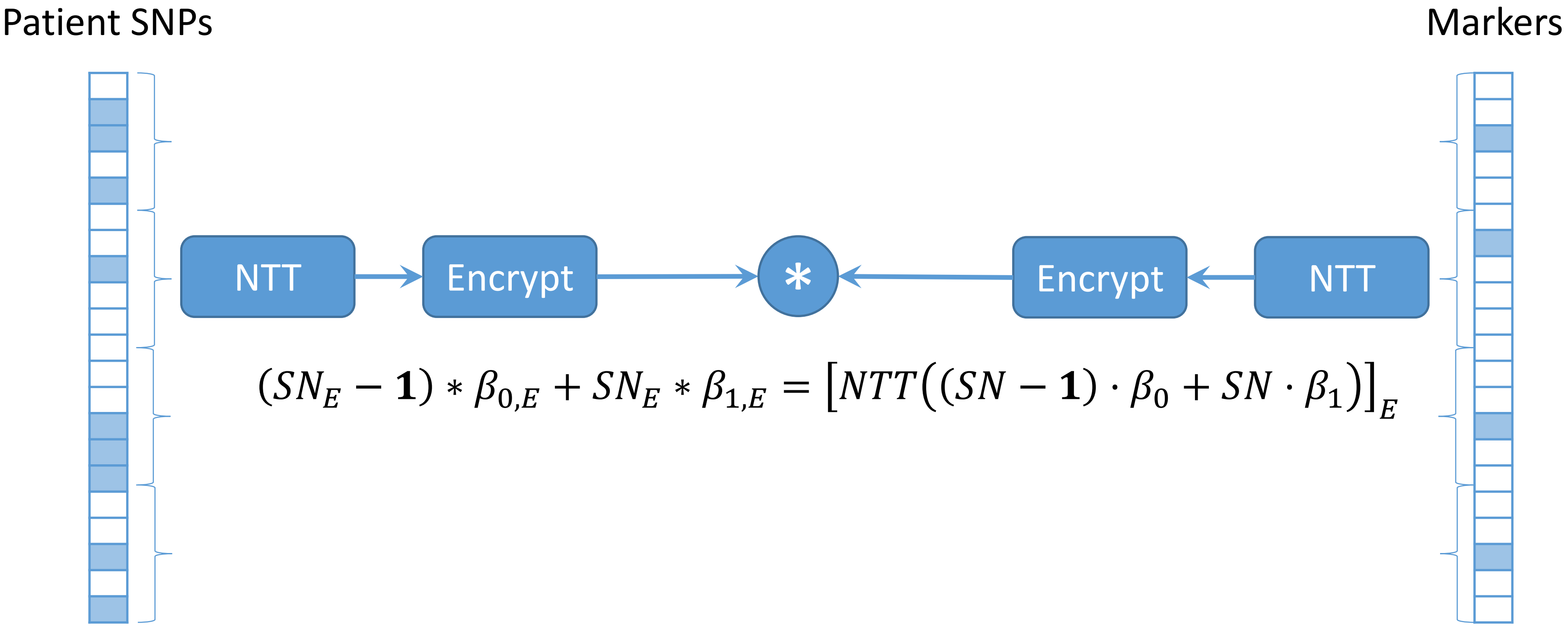


$$\beta_{b,E} = \left(NTT\left[\sum_{i\in\Omega_x} \frac{(-1)^{1-b} c^{X,i} pr_b^{X,i}}{\sum_{i\,\in\Omega_x} c^{X,i}} \cdot z^i \right] \right)_E$$

Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available

$$NTT[\boldsymbol{x}]_k = \sum_{i \in [0,N)} x_i \alpha^{i \cdot k}$$

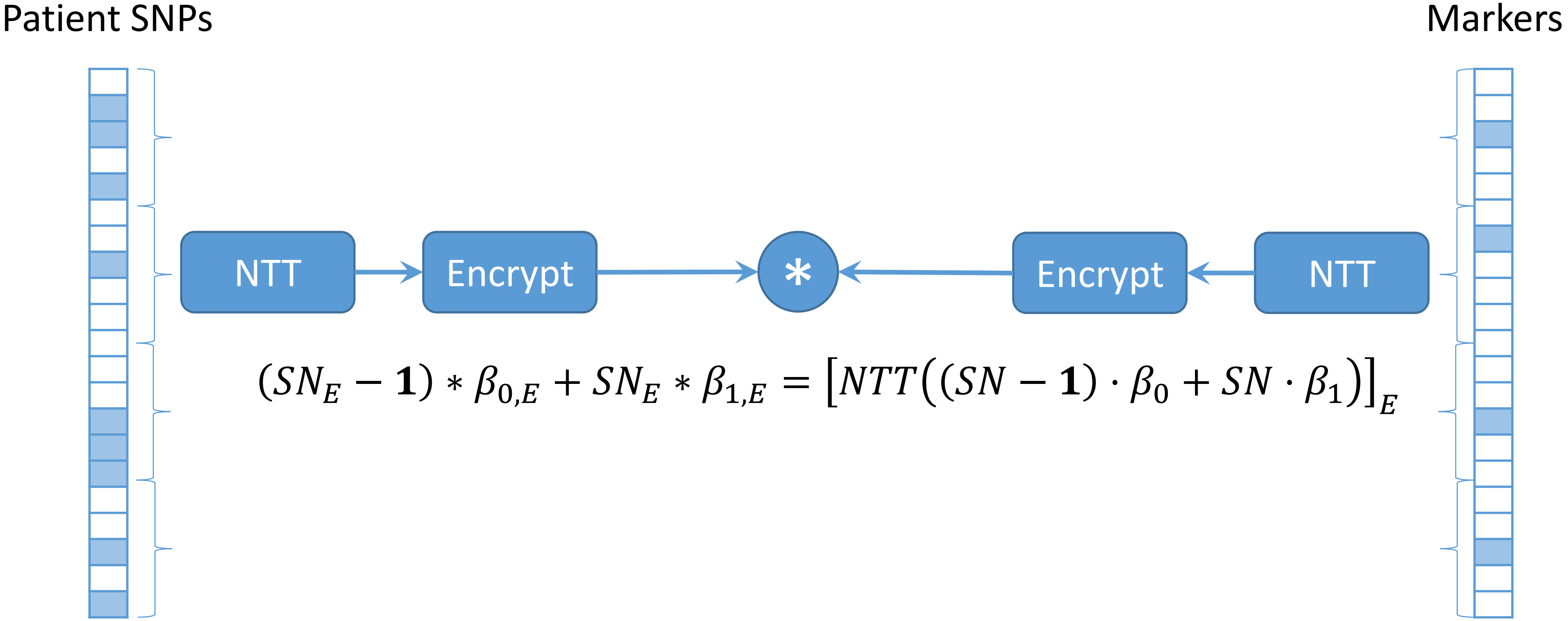


$$(SN_E - \mathbf{1}) * \beta_{0,E} + SN_E * \beta_{1,E} = \left[NTT\big((SN - \mathbf{1}) \cdot \beta_0 + SN \cdot \beta_1\big)\right]_E$$

Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available
  - Recover the sum

$$NTT[\boldsymbol{x}]_k = \sum_{i \in [0,N)} x_i \alpha^{i \cdot k}$$

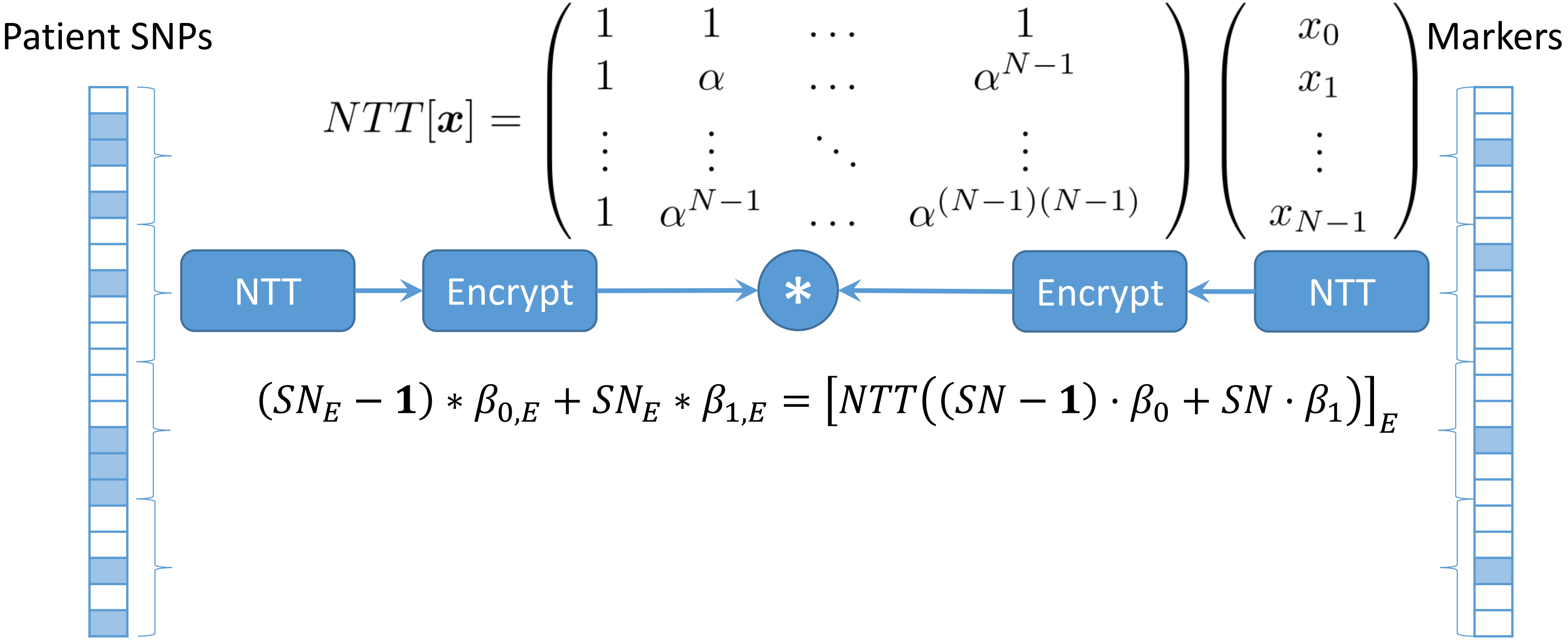


$$(SN_E - \mathbf{1}) * \beta_{0,E} + SN_E * \beta_{1,E} = \left[NTT\left((SN - \mathbf{1}) \cdot \beta_0 + SN \cdot \beta_1\right)\right]_E$$

Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available
  - Recover the sum

$$NTT[\boldsymbol{x}]_k = \sum_{i\in[0,N)} x_i \alpha^{i\cdot k}$$



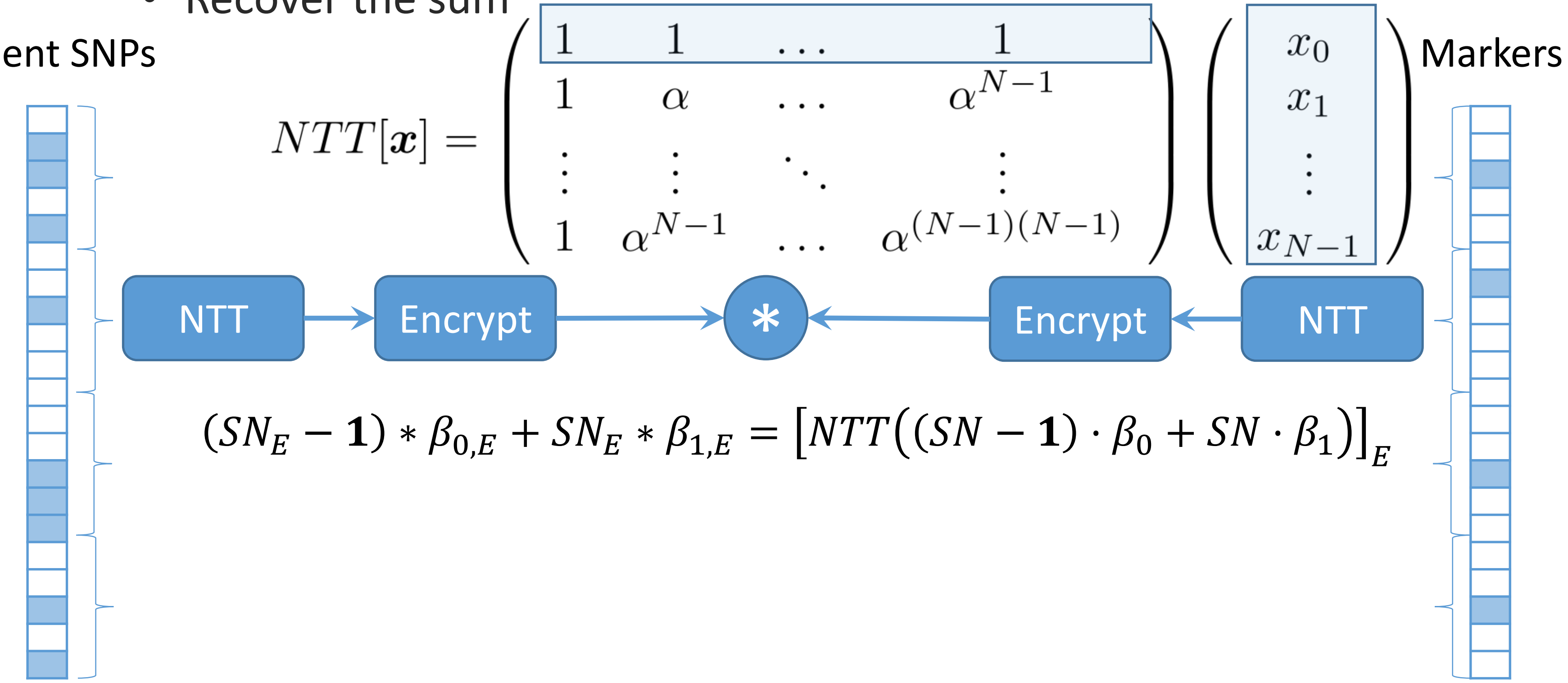
$$NTT[\boldsymbol{x}] = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{N-1} & \dots & \alpha^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}$$

$$(SN_E - \mathbf{1}) * \beta_{0,E} + SN_E * \beta_{1,E} = \left[NTT\big((SN - \mathbf{1}) \cdot \beta_0 + SN \cdot \beta_1\big)\right]_E$$

Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available
  - Recover the sum

$$NTT[\boldsymbol{x}]_k = \sum_{i \in [0,N)} x_i \alpha^{i \cdot k}$$



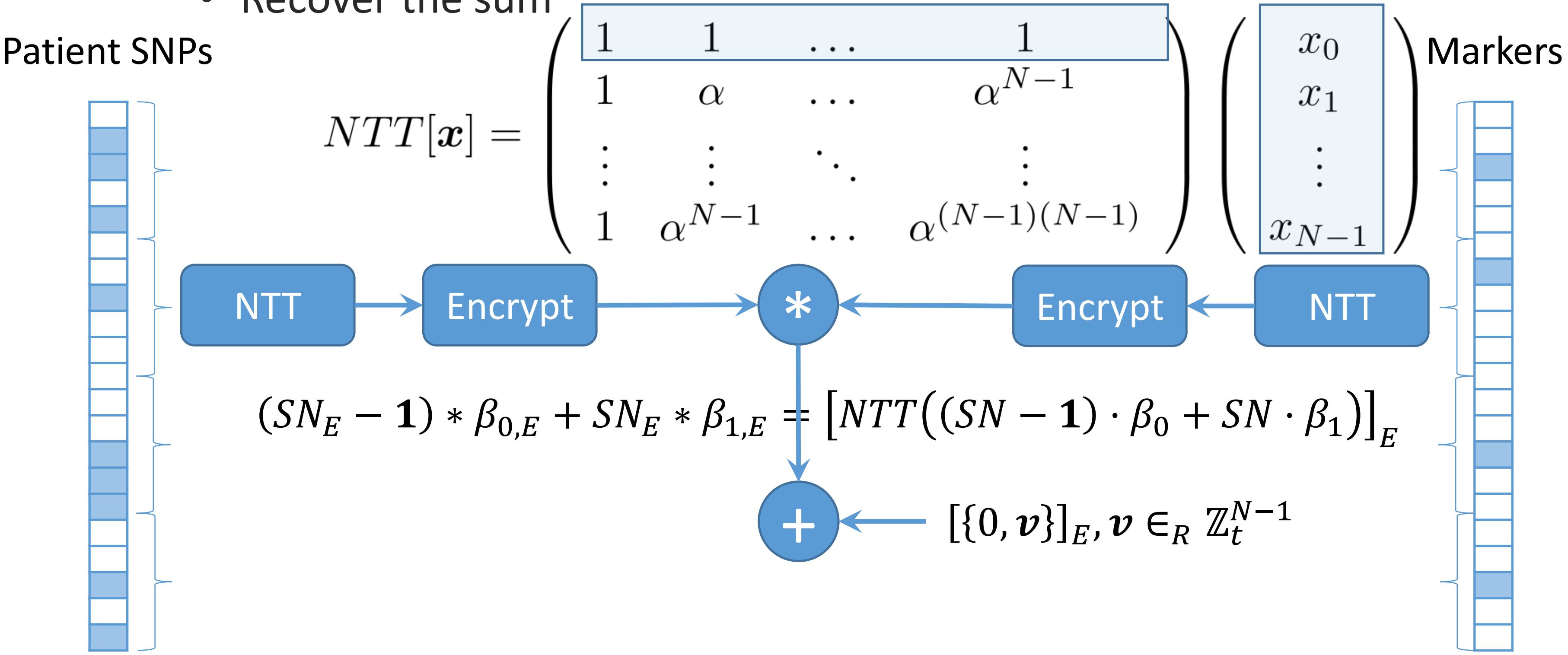
$$NTT[\boldsymbol{x}] = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{N-1} & \dots & \alpha^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}$$

$$(SN_E - \mathbf{1}) * \beta_{0,E} + SN_E * \beta_{1,E} = \left[NTT\left((SN - \mathbf{1}) \cdot \beta_0 + SN \cdot \beta_1\right)\right]_E$$

Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available
  - Recover the sum

$$NTT[\boldsymbol{x}]_k = \sum_{i \in [0,N)} x_i \alpha^{i \cdot k}$$



$$NTT[\boldsymbol{x}] = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{N-1} & \dots & \alpha^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}$$

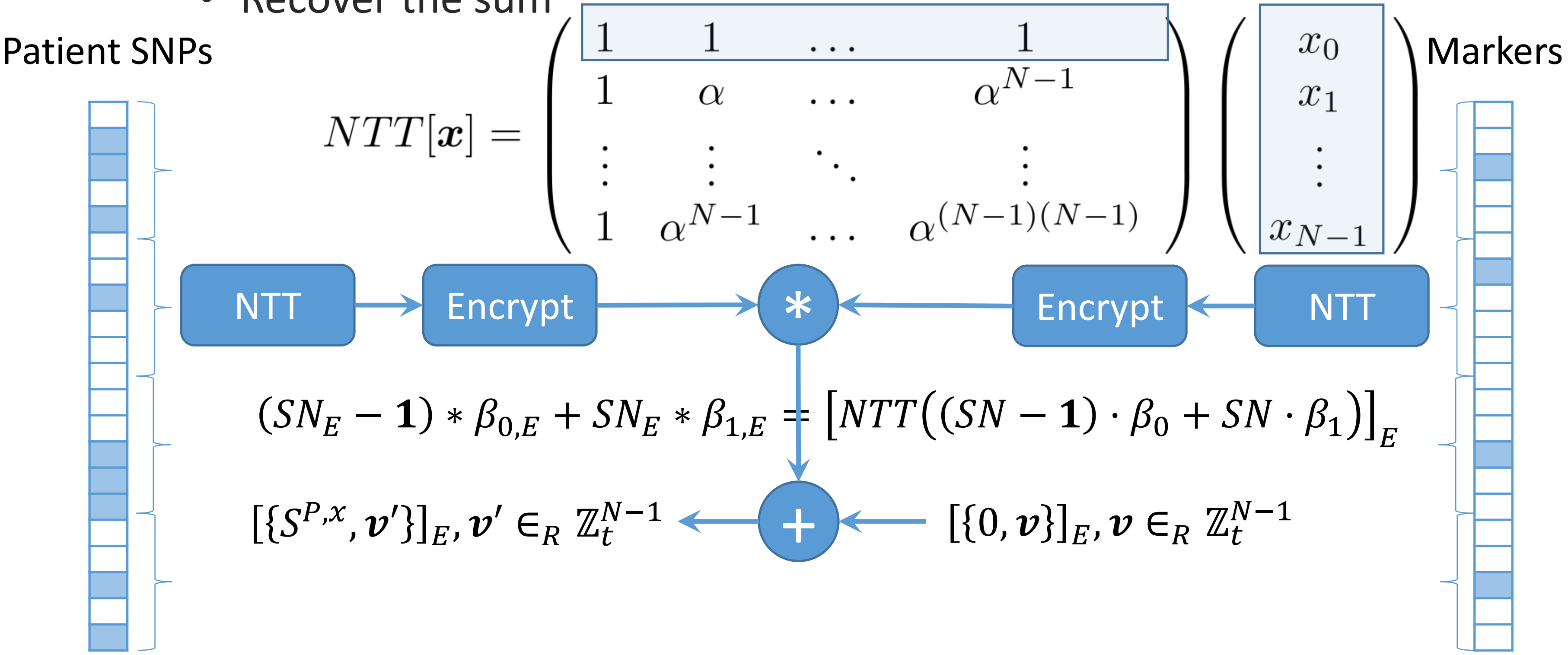
$$(SN_E - \mathbf{1}) * \beta_{0,E} + SN_E * \beta_{1,E} = \left[NTT\left((SN - \mathbf{1}) \cdot \beta_0 + SN \cdot \beta_1\right)\right]_E$$

$$[\{0, \boldsymbol{v}\}]_E, \boldsymbol{v} \in_R \mathbb{Z}_t^{N-1}$$

Privacy-preserving genomic susceptibility testing

- One step further: packing
  - Reduce cipher expansion
  - Needed scalar product, polynomial product available
  - Recover the sum

$$NTT[\boldsymbol{x}]_k = \sum_{i\in[0,N)} x_i \alpha^{i\cdot k}$$



$$NTT[\boldsymbol{x}] = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{N-1} & \dots & \alpha^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}$$

$$(SN_E - \mathbf{1}) * \beta_{0,E} + SN_E * \beta_{1,E} = \left[NTT\left((SN - \mathbf{1}) \cdot \beta_0 + SN \cdot \beta_1\right)\right]_E$$

$$[\{S^{P,x}, \boldsymbol{v}'\}]_E, \boldsymbol{v}' \in_R \mathbb{Z}_t^{N-1}$$

$$[\{0, \boldsymbol{v}\}]_E, \boldsymbol{v} \in_R \mathbb{Z}_t^{N-1}$$

Security and Performance Evaluation

4M SNPs, 10-marker test

Paillier: 2048-bit modulus, 112 bit security
Lauter: 2048-dim. lattice, 127 bit-security (δ = 1.005)

Ayday et al.	CI	SPU		MC	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4.1 GB	10.2 kB	1.02 kB	1.02 kB	

Namazi et al.	CI	SPU		MC	
127 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.22 ms	1.08 ms	1.1 ms	4.5 ms	0.46 ms
Size	131.1 GB		32.8 kB	655 kB	

Proposed	CI	SPU		MC	
127 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.00011 ms	0.05 – 1.08 ms	1.1 ms	0.22 – 4.5 ms	0.46 ms
Size	64 MB		32.8 kB	65.5 - 655 kB	

Paillier: 2048-bit modulus, 112 bit security
Lauter: 2048-dim. lattice, 127 bit-security ($\delta = 1.005$)

Ayday et al.	CI	SPU		MC	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4.1 GB	10.2 kB	1.02 kB	1.02 kB	

Namazi et al.	CI	SPU		MC	
127 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.22 ms	1.08 ms	1.1 ms	4.5 ms	0.46 ms
Size	131.1 GB		32.8 kB	655 kB	

Proposed	CI	SPU		MC	
127 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.00011 ms	0.05 – 1.08 ms	1.1 ms	0.22 – 4.5 ms	0.46 ms
Size	64 MB		32.8 kB	65.5 - 655 kB	

Paillier: 2048-bit modulus, 112 bit security
Lauter: 2048-dim. lattice, 127 bit-security (δ = 1.005)

Ayday et al.	CI	SPU		MC	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4.1 GB	10.2 kB	1.02 kB	1.02 kB	

Namazi et al.	CI	SPU		MC	
127 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.22 ms	1.08 ms	1.1 ms	4.5 ms	0.46 ms
Size	131.1 GB		32.8 kB	655 kB	

Proposed	CI	SPU		MC	
127 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.00011 ms	0.05 – 1.08 ms	1.1 ms	0.22 – 4.5 ms	0.46 ms
Size	64 MB		32.8 kB	65.5 - 655 kB	

Paillier: 2048-bit modulus, 112 bit security
Lauter: 2048-dim. lattice, 127 bit-security ($\delta = 1.005$)

Ayday et al.	**CI**	**SPU**		**MC**	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4.1 GB	10.2 kB	1.02 kB	1.02 kB	
Namazi et al.	**CI**	**SPU**		**MC**	
127 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.22 ms	1.08 ms	1.1 ms	4.5 ms	0.46 ms
Size	131.1 GB		32.8 kB	655 kB	
Proposed	**CI**	**SPU**		**MC**	
127 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.00011 ms	0.05 – 1.08 ms	1.1 ms	0.22 – 4.5 ms	0.46 ms
Size	64 MB		32.8 kB	65.5 - 655 kB	

Paillier: 2048-bit modulus, 112 bit security
Lauter: 4096-dim. lattice, 364 bit-security (δ = 1.002)

Ayday et al.	**CI**	**SPU**		**MC**	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4.1 GB	10.2 kB	1.02 kB	1.02 kB	
Namazi et al.	**CI**	**SPU**		**MC**	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.45 ms	2.17 ms	2.32 ms	9.1 ms	0.96 ms
Size	262.1 GB		65.5 kB	1.31 MB	
Proposed	**CI**	**SPU**		**MC**	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.00011 ms	0.1 – 2.17 ms	2.32 ms	0.45 – 9.1 ms	0.96 ms
Size	64 MB		65.5 kB	0.13 – 1.31 MB	

Paillier: 2048-bit modulus, 112 bit security
Lauter: 4096-dim. lattice, 364 bit-security (δ = 1.002)

Ayday et al.	**CI**	**SPU**		**MC**	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4.1 GB	10.2 kB	1.02 kB	1.02 kB	
Namazi et al.	**CI**	**SPU**		**MC**	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.45 ms	2.17 ms	2.32 ms	9.1 ms	0.96 ms
Size	262.1 GB		65.5 kB	1.31 MB	
Proposed	**CI**	**SPU**		**MC**	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.00011 ms	0.1 – 2.17 ms	2.32 ms	0.45 – 9.1 ms	0.96 ms
Size	64 MB		65.5 kB	0.13 – 1.31 MB	

Paillier: 2048-bit modulus, 112 bit security
Lauter: 4096-dim. lattice, 364 bit-security ($\delta = 1.002$)

Ayday et al.	**CI**	**SPU**		**MC**	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4.1 GB	10.2 kB	1.02 kB	1.02 kB	
Namazi et al.	**CI**	**SPU**		**MC**	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.45 ms	2.17 ms	2.32 ms	9.1 ms	0.96 ms
Size	262.1 GB		65.5 kB	1.31 MB	
Proposed	**CI**	**SPU**		**MC**	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.00011 ms	0.1 – 2.17 ms	2.32 ms	0.45 – 9.1 ms	0.96 ms
Size	64 MB		65.5 kB	0.13 – 1.31 MB	

Paillier: 2048-bit modulus, 112 bit security
Lauter: 4096-dim. lattice, 364 bit-security ($\delta = 1.002$)

Ayday et al.	CI	SPU		MC	
112 bit security	Encrypt/ SNP	Recrypt	Proxy recrypt	Homomorphic calculation	Paillier decrypt
Time	33.2 ms	304.3 ms	30.3 ms	39.3 ms	30.3 ms
Size	4.1 GB	10.2 kB	1.02 kB	1.02 kB	
Namazi et al.	**CI**	**SPU**		**MC**	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.45 ms	2.17 ms	2.32 ms	9.1 ms	0.96 ms
Size	262.1 GB		65.5 kB	1.31 MB	
Proposed	**CI**	**SPU**		**MC**	
364 bit security	Encrypt/ SNP	Homomorphic calculation	Relineariz	Enc params	Decrypt
Time	0.00011 ms	0.1 – 2.17 ms	2.32 ms	0.45 – 9.1 ms	0.96 ms
Size	64 MB		65.5 kB	0.13 – 1.31 MB	

Conclusions

Conclusions

- An efficient protocol to deal with encrypted genomic susceptibility tests is proposed
- We introduce some optimizations:
  - A reasonable choice of the cryptosystem parameters (for both efficiency and security)
  - A transformed input packing strategy
  - Avoiding costly unpacking/repacking operations
- It moves the bulk of the computation to the SPU
- It outperforms previous solutions in both computational cost, bandwidth and storage

AtlantTIC

Research Center for
Information & Communication Technologies

Thanks for your attention!