Fully homomorphic encryption scheme using ideal lattices

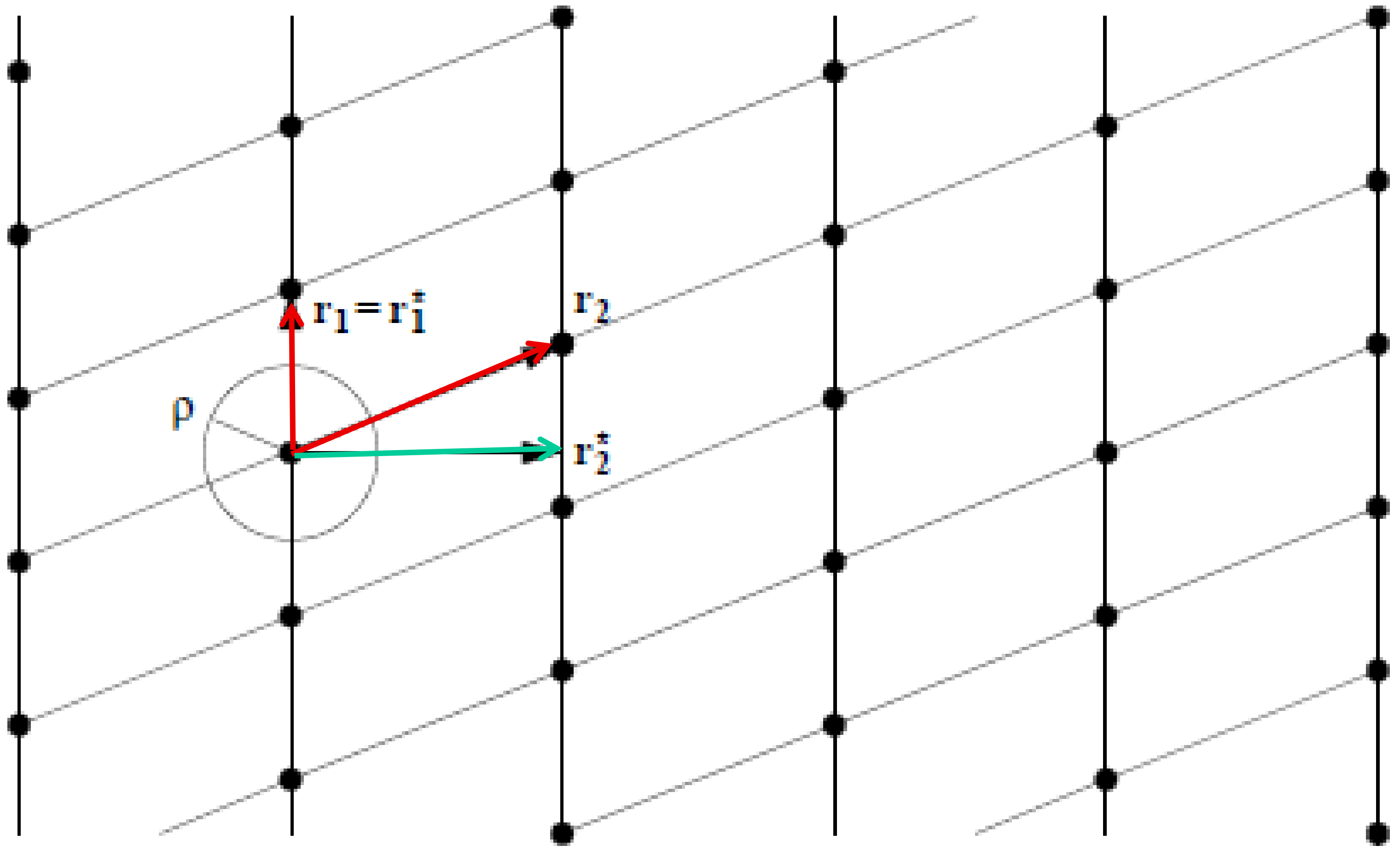
Gentry’s STOC’09 paper - Part II

GGH cryptosystem

- Gentry’s scheme is a GGH-like scheme.
- GGH: Goldreich, Goldwasser, Halevi.
- Based on the hardness of ClosestVector Problem (CVP).
- Our discussion of GGH is variant by D. Micciancio: "Improving lattice based cryptosystems using the Hermite normal form," Cryptography and Lattices 2001.

Secret key

- The sceret key is a "good" basis $\mathbf{R} = (\mathbf{r}_1, \ \ldots, \ \mathbf{r}_n)$ of a lattice L.
  - For computational purpose, assume $L \subset \mathbb{Z}^n$.
  - The quantity $\rho_{\mathbf{R}} = \frac{1}{2}\min\left\|\mathbf{r}_i^*\right\|$ is relatively large.
  - We know: $\lambda_1(L) \geq \min\left\|\mathbf{r}_i^*\right\|$; thus, $\lambda_1(L) \geq 2\rho_{\mathbf{R}}$.
  - Thus, the orthogonalized centered parallelepiped $C(\mathbf{R}^*)$ is fat, containing a ball of radius $\rho_{\mathbf{R}}$.
  - Any point $\mathbf{t} \in \mathbb{Z}^n$ with $\mathrm{dist}(\mathbf{t}, L) < \rho_{\mathbf{R}}$ can be corrected to the closest lattice point (using the nearest plane algorithm).

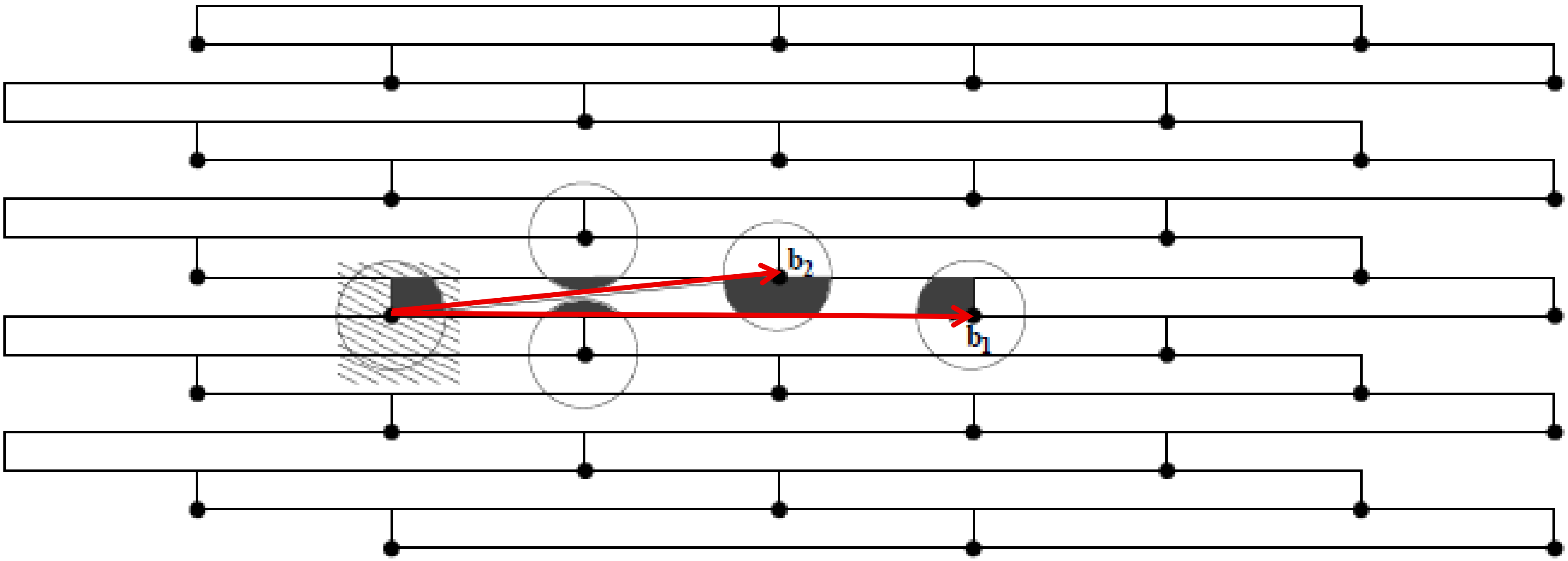


A good basis and the corresponding correction radius

Source: Daniele Micciancio's paper, CaLC 2001

Public key

- The public key is a "bad" basis $\mathbf{B} = \left(\mathbf{b}_1, \ \ldots, \ \mathbf{b}_n\right)$ of L.
  - For example, $\mathbf{B} = \mathrm{HNF}(\mathbf{R})$.
  - Its orthogonalized parallelepiped, $P(\mathbf{B}^*)$, is skiny.
  - $\rho_{\mathbf{B}} = \frac{1}{2}\min\left\|\mathbf{b}_i^*\right\|$ is much smaller than $\rho_{\mathbf{R}}$.
  - CVP (BDDC) is hard (w/o knowing $\mathbf{R}$) even if $\mathrm{dist}\left(\mathbf{t}, L\right) < \rho_{\mathbf{R}}$.
  - Denote by $\mathbf{t} \bmod \mathbf{B}$ the unique $\mathbf{s} \in P(\mathbf{B}^*)$ s.t.
    $\mathbf{s}$ is congruent to $\mathbf{t}$ modulo L (i.e., $\mathbf{s} \equiv_L \mathbf{t}$ or $\mathbf{t} - \mathbf{s} \in L$).
  - (Here we use $P(\mathbf{B}^*)$ as the representative system of $\mathbb{R}^n / L$.)

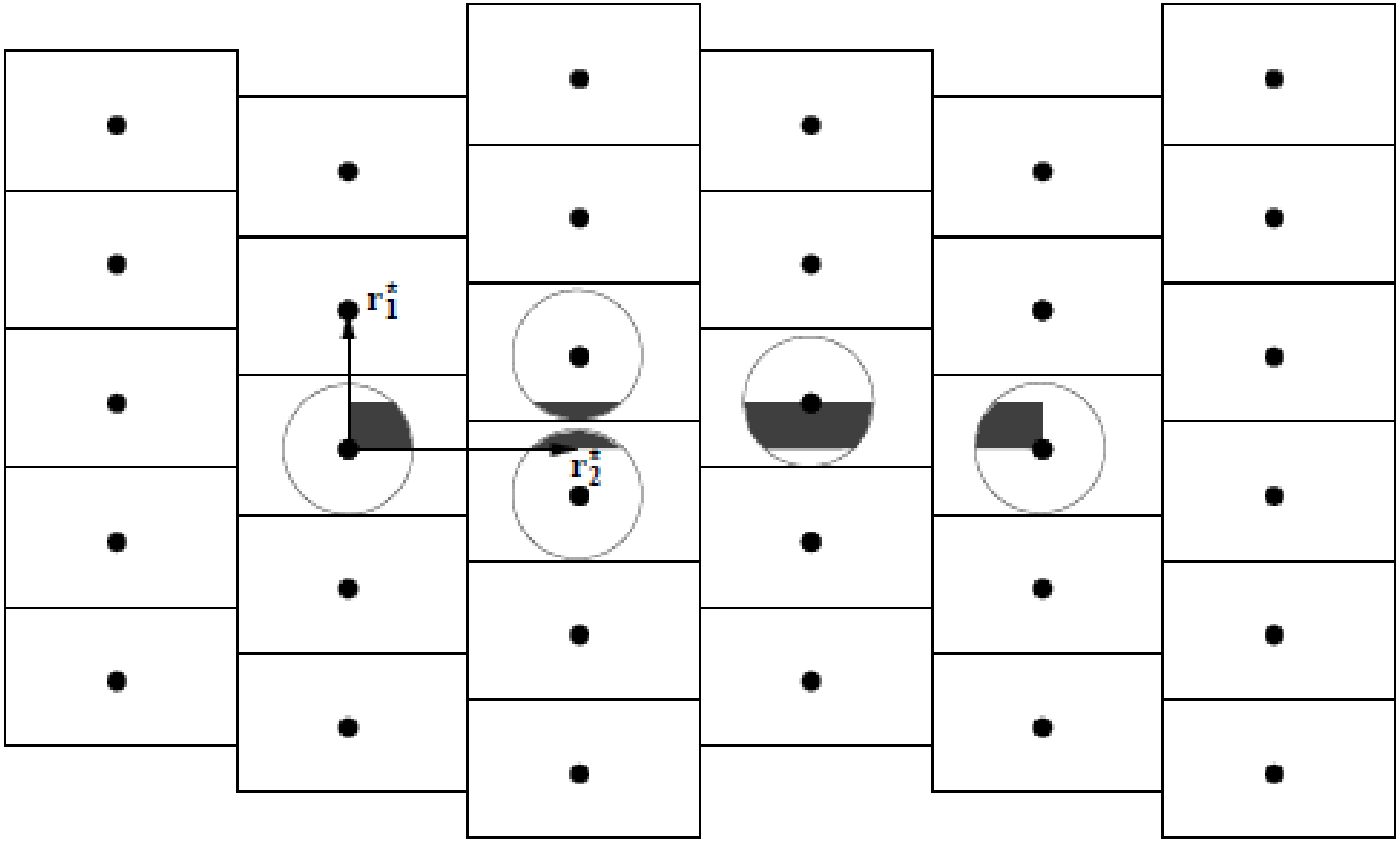


HNF basis and corresponding orthogonalized parallelepiped

Source: Daniele Micciancio's paper, CaLC 2001

Encryption and Decryption

- Encryption: to encrypt a message m,
  - Encode m as a vector $\mathbf{r}$, $\|\mathbf{r}\| < \rho_{\mathbf{R}}$.
  - $\mathbf{c} \leftarrow \mathbf{r} \bmod \mathbf{B}$.
- Decryption: to decrypt a ciphertext $\mathbf{c}$,
  - Recover $\mathbf{r}$ from $\mathbf{c}$ by $\mathbf{r} \leftarrow \mathbf{c} \bmod \mathbf{R}$.
  - Recover m from $\mathbf{r}$.



Correcting small errors using the private basis

From Micciancio's paper

Is GGH homomorphic?

- If the encoding scheme is such that

$$\left.\begin{aligned} m_1 &\to \mathbf{r}_1 \\ m_2 &\to \mathbf{r}_2 \end{aligned}\right\} \Rightarrow \quad m_1 + m_2 \to \mathbf{r}_1 + \mathbf{r}_2$$

  and if $\|\mathbf{r}_1\|, \|\mathbf{r}_2\| < \rho_{\mathbf{R}}/2$, then GGH is additively homomorphic:

$$\mathrm{GGH}(m_1 + m_2) = \mathrm{GGH}(m_1) +_{\mathrm{mod}\,\mathbf{B}} \mathrm{GGH}(m_2)$$

- How to make it multiplicatively homomorphic?
  - Genty's answer: use ideal lattices.

Ideals

Gentry's scheme uses ideal lattices, which are lattices corresponding to some ideals

Rings

- A ring R is a set together with two binary operations + and $\times$ satisfying the following axioms:
  - $(R,+)$ is an abelian group.
  - $\times$ is associative: $(a\times b)\times c = a\times(b\times c)$ for all $a,b,c\in R$.
  - Distributive laws hold: $(a+b)\times c=(a\times c)+(b\times c)$ and $a\times(b+c)=(a\times b)+(a\times c)$.
- The ring R is commutative if $a\times b=b\times a$.
- The ring R is said to have an identity if there is an element $1\in R$ with $a\times 1=1\times a=a$ for all $a\in R$.
- We will only be interested in communative rings with an identy.

Ideals

- An ideal I of a ring R is an additive subgroup of R s.t. $r \times I \subseteq I$ for all $r \in R$. (I.e., a subset $I \subseteq R$ s.t. $a - b \in I$ and $r \times a \in I$ for all $a,\ b \in I,\ r \in R$.)
- Example:
  - Consider the ring $\mathbb{Z}$.
  - For any integer a, $I_a = \{na : n \in \mathbb{Z}\}$ is an ideal.
  - Conversely, any ideal $I \subseteq \mathbb{Z}$ is equal to I_a for some $a \in \mathbb{Z}$.
  - The mapping $f:\ a \mapsto I_a$ is a bijective function from $\{\text{nonnegative integers}\} \to \{\text{ideals of } \mathbb{Z}\}$.
- The name ideal comes from "ideal" numbers.

Some historical notes

- An algebraic integer is a number $x \in \mathbb{C}$ satisfying
  $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$ where $a_i \in \mathbb{Z}$.

- The set of all algebraic integers forms a ring.

- For any algebraic integer α, $\mathbb{Z}[\alpha]$ denote the closure of $\mathbb{Z} \cup \{\alpha\}$ under $+, \ -, \ \times$.

- Example: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Gaussian integers.

- $\mathbb{Z}[\alpha]$ resembles $\mathbb{Z}$, and many questions concerning $\mathbb{Z}$ can be answered by considering $\mathbb{Z}[\alpha]$.

- For instance, Format's theorem on sums of two squares: an odd prime p can be expressed as $p = x^2 + y^2 \ (x, y \in \mathbb{Z})$ iff $p \equiv 1 \bmod 4$.
- This theorem can be proved by showing that in $\mathbb{Z}[i]$
  - if $p \equiv 1 \bmod 4,$ then p factors into $p = (a+bi)(a-bi)$
  - if $p \equiv 3 \bmod 4,$ then p cannot be factored.
- While $\mathbb{Z}$ has the unique prime factorization property, $\mathbb{Z}[\alpha]$ in general doesn't. For instance, in $\mathbb{Z}\left[\sqrt{-5}\right],$ 6 has two prime factorizations: $6 = 2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right).$

- Eduard Kummer, inspired by the discovery of imaginary numbers, introduced ideal numbers.
- For instance, in the example of $6 = 2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$, we may define ideal prime numbers $p_1,\ p_2,\ p_3,\ p_4$, which are subject to the rules:

  $$p_1 p_2 = 2, \quad p_3 p_4 = 3, \quad p_1 p_3 = 1+\sqrt{-5}, \quad p_2 p_4 = 1-\sqrt{-5}.$$

- Then, 6 would have the unique prime factorization:

  $$6 = p_1 p_2 p_3 p_4.$$

- Kummer's concept of ideal numbers was later replaced by that of ideals, by Richard Dedekind.

Operations on Ideals

- Let $I,\ J$ be ideals of the ring R.
- Sum of ideals: $I + J \triangleq \{a+b:\ a \in I,\ b \in J\}$, which is the smallest ideal containing both I and J.
- Product of ideals: $I \times J \triangleq$ the set of all finite sums of the form $a \times b$ with $a \in I,\ b \in J$. I.e., the smallest ideal containing $\{a \times b:\ a \in I,\ b \in J\}$. Thus, R is the identy.
- I divides J iff $I \supseteq J$. Thus, $\gcd(I, J) = (I, J) = I + J$.
- I is a prime ideal if $\forall a, b \in R, ab \in I \Rightarrow a \in I$ or $b \in I$.
- Two ideal I and J are relatively prime if $I + J = R$.

Generators and Bases of ideals

- Let B be any subset of a ring R.
- Denote by (B) the smallest ideal of R containing B, called the ideal generated by B. We have:
  $(B) = \left\{ r_1 b_1 + \cdots + r_n b_n : \; r_i \in R, \; b_i \in B, \; n \in \mathbb{Z}^+ \right\}$
- The ideal $I = (B)$ is finitely generated if B is finite, and is a principal ideal if B contains a single element.
- B is a basis of $I = (B)$ if it is linearly independent.

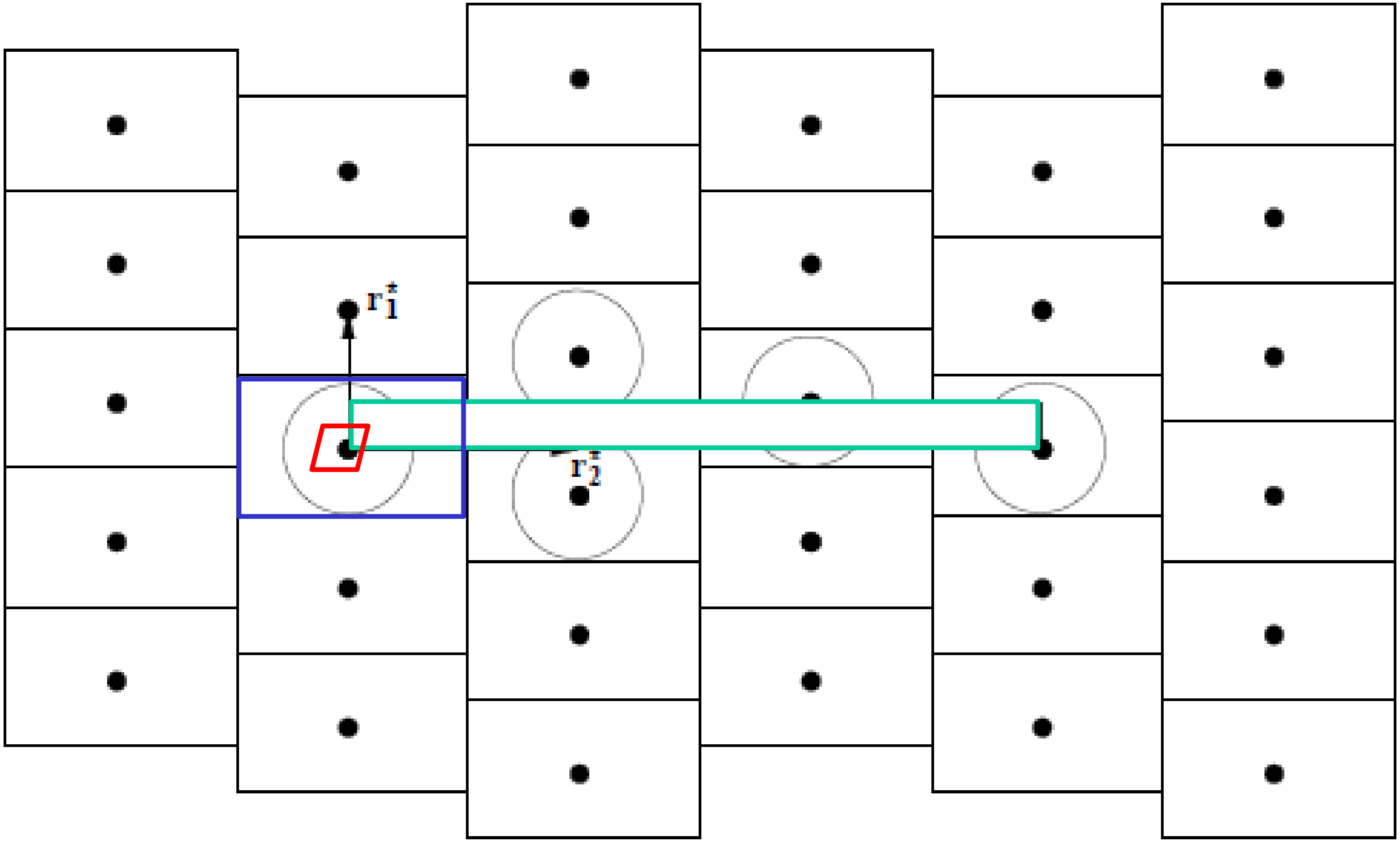
Cosets

- Let I be an ideal of a ring R.
- R is partitioned into cosets s.t. two elements $a,\ b \in R$ are in the same coset iff $a-b \in I$. $R = \bigcup_{a \in Z} (I+a)$
- The coset containing a is $[a]_I = a + I = \{a+i : i \in I\}$.
- Define $[a]_I + [b]_I = [a+b]_I$ and $[a]_I \times [b]_I = [a \times b]_I$.
- The cosets form a ring R/I, called the quotient ring.
- Choose an element from each coset as a representative, then we have a system of representatives for R/I. For $x \in R,$ denote by $x \bmod I$ the element representing $[x]_I$.

Gentry’s Ideal-based Scheme

Notations

- Let I be an ideal of the ring R, and $\mathbf{B}_I$ a basis of I.
- $R \bmod \mathbf{B}_I$: a system of representatives for R/I defined by $\mathbf{B}_I$.
- If $\mathbf{B}_1 \neq \mathbf{B}_2$ are two bases for the same ideal, we have in general $\mathbf{x} \bmod \mathbf{B}_1 \neq \mathbf{x} \bmod \mathbf{B}_2$ (not necessarily equal).
- $\text{Samp}(\mathbf{x}, \mathbf{B}_I)$: samples the coset $\mathbf{x} + I$ according to some probability distribution.
- C : a circuit whose gates perform + and $\times$ operations mod $\mathbf{B}_I$.
- $g(C)$: generalized C, the same as C but without mod $\mathbf{B}_I$.
- $C_{\mathbf{B}_J}$: same as C, but gates perform mod $\mathbf{B}_J$ operations instead.



From Micciancio's paper

Σ: an ideal-based encryption scheme

- KeyGen$(R, \mathbf{B}_I)$:
  - Input: a ring R, a basis $\mathbf{B}_I$ of an ideal I.
  - $(\mathbf{B}_J^{\text{sk}}, \mathbf{B}_J^{\text{pk}}) \leftarrow_{\text{R}} \text{IdealGen}(R, \mathbf{B}_I)$.
  - Public key $pk := \mathbf{B}_J^{\text{pk}}$. Secret key $sk := \mathbf{B}_J^{\text{sk}}$.
  - Parameters: $(R, \mathbf{B}_I, \text{Samp})$, which are public info.
  - Plaintext space $P :=$ (a subset of) R mod $\mathbf{B}_I$

- Remarks: As in GGH, $\mathbf{B}_J^{\text{sk}}$ is a good (fat) basis and $\mathbf{B}_J^{\text{pk}}$ a bad (skiny) one. The ideal I is used to encode plaintexts as ring elements.

- Encrypt(pk, π): $//\pi \in P//$

  $\pi' \leftarrow \mathrm{Samp}(\pi, \mathbf{B}_I)$ // an element in coset $\pi + I$ //

  $\psi \leftarrow \pi' \bmod \mathbf{B}_J^{\mathrm{pk}}$ // the ciphertext //

- Decrypt(sk, ψ):

  $\pi \leftarrow \left(\psi \bmod \mathbf{B}_J^{\mathrm{sk}}\right) \bmod \mathbf{B}_I$

- Remarks:
  - π is encoded as a random element π' in the same coset.
  - π' is then encrypted as in GGH.
  - Decryption is correct if $\pi' \in R \bmod \mathbf{B}_J^{\mathrm{sk}}$.

- Evaluate$\left(pk, C, \Psi\right)$:
  - Input: a public key pk; a mod $\mathbf{B}_I$ circuit C composed of $\text{Add}_{\mathbf{B}_I}$ and $\text{Mult}_{\mathbf{B}_I}$ (and identity) gates; and ciphertexts $\Psi = (\psi_1, \ldots, \psi_t)$, where $\psi_i = \text{Encrypt}\left(pk, \pi_i\right)$, $\pi_i \in P$.
  - Output: $\psi := g(C)\left(\Psi\right) \bmod \mathbf{B}_J^{pk}$. $// = g(C)\left(\Pi'\right) \bmod \mathbf{B}_J^{pk} //$
- Remarks:
  - Evaluate$\left(pk, \text{Add}_{\mathbf{B}_I}, \psi_1, \psi_2\right)$: outputs $\psi_1 + \psi_2 \bmod \mathbf{B}_J^{pk}$.
  - Evaluate$\left(pk, \text{Mult}_{\mathbf{B}_I}, \psi_1, \psi_2\right)$: outputs $\psi_1 \times \psi_2 \bmod \mathbf{B}_J^{pk}$.
  - Evaluate circuit C by evaluating its gates in a proper order.

Correctness: informal

- Evaluating C yields:

$$\psi := C_{\mathbf{B}_J^{pk}}(\Psi) = g(C)(\Psi) \bmod \mathbf{B}_J^{pk} = g(C)(\Pi') \bmod \mathbf{B}_J^{pk}$$

where $\Pi = (\pi_1, \ldots, \pi_t) \xrightarrow{\text{encode}} \Pi' = (\pi_1', \ldots, \pi_t')$

$$\xrightarrow{\bmod \mathbf{B}_J^{pk}} \Psi = (\psi_1, \ldots, \psi_t).$$

- Decrypting ψ will yield: $\pi := (\psi \bmod \mathbf{B}_J^{\text{sk}}) \bmod \mathbf{B}_I$.
- Correct if $g(C)(\Pi') \in R \bmod \mathbf{B}_J^{\text{sk}}$.
- Thus, if we restrict $\pi_1', \ldots, \pi'$ to be in certain region, the scheme will be homomorphic for circuits C for which $g(C)(\Pi') \in R \bmod \mathbf{B}_J^{\text{sk}}$.

Correctness of the ideal-based scheme Σ

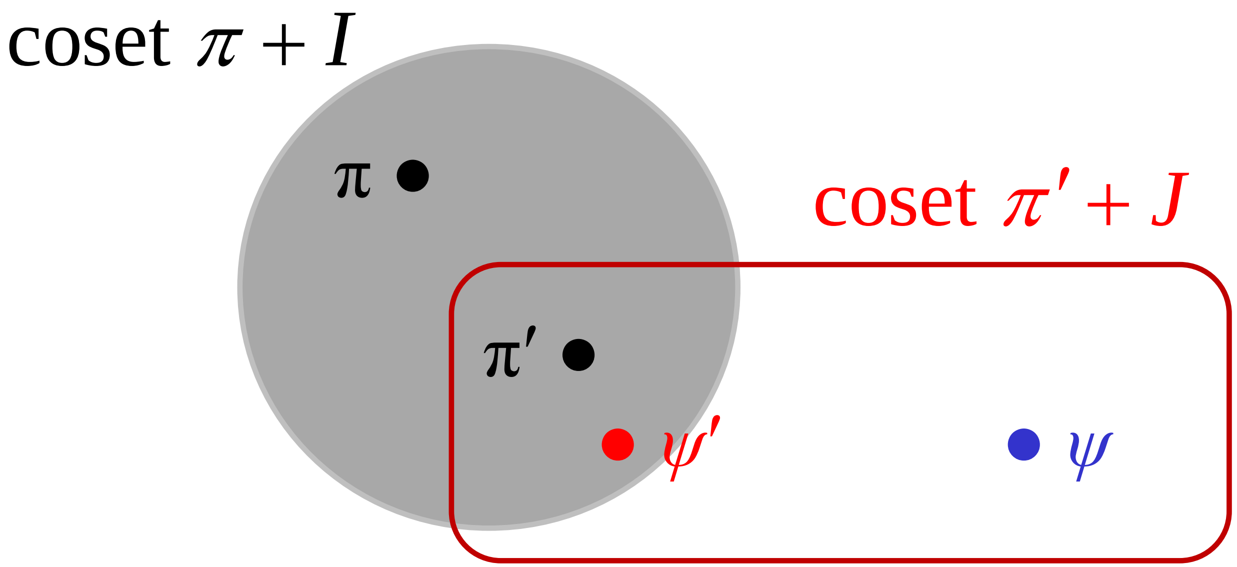
- Let $X_{Enc} \triangleq \mathrm{Samp}\left(\mathbf{B}_I, M\right)$ and $X_{Dec} \triangleq R \bmod \mathbf{B}_J^{pk}$.
- A $\bmod \mathbf{B}_I$ circuit C (including the identity circuit) with $t \geq 1$ inputs is a permitted circuit w.r.t. the scheme if:

$$\forall\, x_1, \ldots, x_t \in X_{Enc},\; g(C)\left(x_1, \ldots, x_t\right) \in X_{Dec}.$$

- Theorem: If C_Σ is a set of permitted circuits containing the identity circuit, then the scheme is correct for C_Σ.
  - I.e., algorithm Decrypt correctly decrypts valid ciphertexts:

    $C\left(\Pi\right) = \mathrm{Decrypt}\left(sk, \mathrm{Evaluate}\left(pk, C, \Psi\right)\right)$,

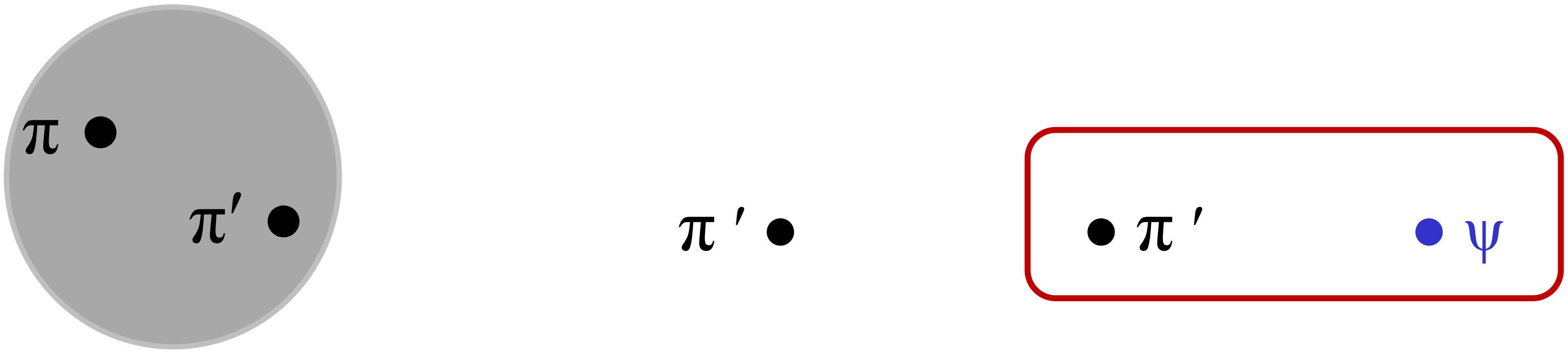
    where $C \in C_\Sigma$ and $\Psi \leftarrow \mathrm{Encrypt}\left(sk, \Pi\right)$.
  - Valid ciphertexts: outputs of $\mathrm{Evaluate}\left(pk, C, \Psi\right)$, $C \in C_\Sigma$.



Encrypt: $\pi \xrightarrow{\text{Samp}(\mathbf{B}_I,\ \pi)} \pi' \xrightarrow{\bmod \mathbf{B}_J^{\text{pk}}} \psi$

Decrypt: $\pi \xleftarrow{\bmod \mathbf{B}_I} \psi' \xleftarrow{\bmod \mathbf{B}_J^{\text{sk}}} \psi$

It works if $\pi' = \psi'$, i.e. if $\pi' \in R \bmod \mathbf{B}_J^{\text{sk}}$.



$C(\Pi)$ $\qquad$ $g(C)(\Pi')$ $\qquad$ $C_{\mathbf{B}_J^{pk}}(\Psi)$

Q: Is $C(\Pi) = \text{Decrypt}\left(sk,\, C_{\mathbf{B}_J^{pk}}(\Psi)\right) \triangleq \left(C_{\mathbf{B}_J^{pk}}(\Psi) \bmod \mathbf{B}_J^{sk}\right) \bmod \mathbf{B}_I$?

$$C(\Pi) = \qquad g(C)(\Pi') \bmod \mathbf{B}_I$$

$$g(C)(\Pi') \bmod \mathbf{B}_J^{pk} = C_{\mathbf{B}_J^{pk}}(\Psi)$$

$$g(C)(\Pi') \bmod \mathbf{B}_J^{sk} = C_{\mathbf{B}_J^{pk}}(\Psi) \bmod \mathbf{B}_J^{sk}$$

$$\left(g(C)(\Pi') \bmod \mathbf{B}_J^{sk}\right) \bmod \mathbf{B}_I = \left(C_{\mathbf{B}_J^{pk}}(\Psi) \bmod \mathbf{B}_J^{sk}\right) \bmod \mathbf{B}_I$$

Yes, if $g(C)(\Pi') = g(C)(\Pi') \bmod \mathbf{B}_J^{sk}$, i.e., $g(C)(\Pi') \in R \bmod \mathbf{B}_J^{sk}$.

Security of the ideal-based scheme

Ideal Coset Problem (ICP)

- Let R be a ring, I an ideal, and $\mathbf{B}_I$ a basis.
- IdealGen: an algorithm that given $(R, \mathbf{B}_I)$ outputs two bases $\mathbf{B}_J^{\mathrm{sk}}$, $\mathbf{B}_J^{\mathrm{pk}}$ of the same ideal J.
- Samp_1: a random algorithm that samples R (non-uniformly).
- Ideal Coset Problem: Fix R, $\mathbf{B}_I$, IdealGen, Samp_1.
  - Challenger: $\left(\mathbf{B}_J^{\mathrm{sk}}, \mathbf{B}_J^{\mathrm{pk}}\right) \leftarrow_{\mathrm{R}} \mathrm{IdealGen}\left(R, \mathbf{B}_I\right)$. $b \leftarrow_{\mathrm{u}} \{0,1\}$.

    If $b = 0$, then $\mathbf{r} \leftarrow_{\mathrm{R}} \mathrm{Samp}_1(R)$, $\mathbf{t} \leftarrow \mathbf{r} \bmod \mathbf{B}_J^{\mathrm{pk}}$.

    If $b = 1$, then $\mathbf{t} \leftarrow_{\mathrm{uniformly}} R \bmod \mathbf{B}_J^{\mathrm{pk}}$.
  - Adversary: given $\mathbf{t}$ and $\mathbf{B}_J^{\mathrm{pk}}$, determine if $b = 0$ or 1.

- Essentially, the problem is to to distinguish between:
  - $b=0$: a coset $[\mathbf{t}]_J$ is chosen according to some "Samp_1".
  - $b=1$: a coset $[\mathbf{t}]_J$ is chosen uniformly randomly.
- The hardness of ICP depends on Samp_1.
- How does ICP connect to Gentry's encryption scheme Σ?
  - A ciphertext is essentially a coset $[\boldsymbol{\pi}']_J$ chosen by Samp.
  - Σ is semantically secure if the ciphertext is random-like.
  - ICP is hard if coset $[\mathbf{t}]_J$ chosen by Samp_1 is random-like.
- Will show ICP $\leq$ distinguishing ciphertexts of scheme Σ.
- Will use Samp_1 to define Samp.

Connect Samp to Samp_1

- $\mathbf{r} \leftarrow \text{Samp}_1(R)$ samples an element in ring R.
- $\mathbf{x}' \leftarrow \text{Samp}\left(\mathbf{x}, \mathbf{B}_I\right)$ samples an element in coset $\left[\mathbf{x}\right]_I$.
- Wanted:

$$\mathbf{r} \text{ random } \Rightarrow \mathbf{x}' \text{ random}$$

- Let $I = \left(\mathbf{s}\right) = R \times \mathbf{s}$ be a principal ideal generated by $\mathbf{s}$.

  Then, $\left[\mathbf{x}\right]_I = \mathbf{x} + R \times \mathbf{s}$.

- Let $\text{Samp}\left(\mathbf{x}, \mathbf{B}_I\right) \triangleq \mathbf{x} + \text{Samp}_1\left(R\right) \times \mathbf{s}$.

Security of the ideal-based scheme Σ

- The Ideal Coset Problem is to distinguish between
  - $\mathbf{t} \leftarrow \text{Samp}_1(R) \bmod \mathbf{B}_J^{pk}$
  - $\mathbf{t} \leftarrow \text{uniform}\left(R \bmod \mathbf{B}_J^{pk}\right)$.

- $\text{Encrypt}(pk, \boldsymbol{\pi})$:

$$\psi \leftarrow \text{Samp}\left(\boldsymbol{\pi}, \mathbf{B}_I\right) \bmod \mathbf{B}_J^{\text{pk}}$$

$$\left(\boldsymbol{\pi} + \text{Samp}_1(R) \times \mathbf{s}\right) \bmod \mathbf{B}_J^{\text{pk}}$$

where $I = (\mathbf{s}) = R \times \mathbf{s}$ is a principal ideal generated by $\mathbf{s}$.

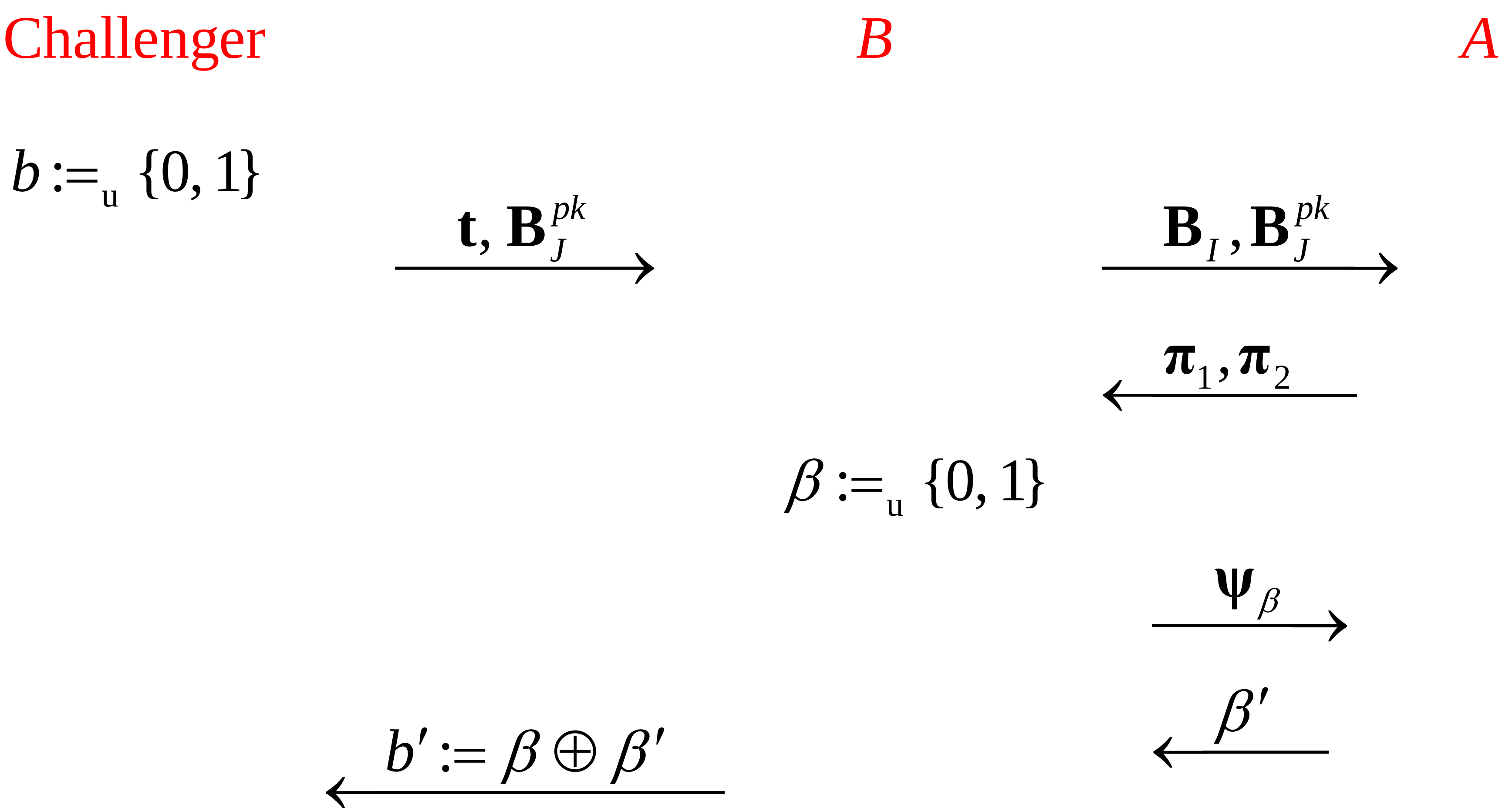
Theorem: If there is an algorithm A that breaks the semantic security of Σ with advantage ε when it uses Samp, then there is an algorithm B, running in about the same time as A, that solves the ICP with advantage $\varepsilon/2$.

Proof: The challenger of ICP sends B an instance $\left(\mathbf{t}, \mathbf{B}_J^{pk}\right)$. B chooses an ideal $I = (\mathbf{s})$ relatively prime to J and sets up the other parameters of Σ. We have two games:

(1) the ICP game between Challenger and B (adversary), and

(2) the Σ game between B (challenger) and A (adversary).

They run as follows.



where if $b = 0$, $\mathbf{t} \leftarrow \mathrm{Samp}_1(R) \bmod \mathbf{B}_J^{pk}$; else, $\mathbf{t} \leftarrow_{\mathrm{u}} R \bmod \mathbf{B}_J^{pk}$; and $\boldsymbol{\psi}_\beta \leftarrow \underbrace{\left(\boldsymbol{\pi}_\beta + \mathbf{t} \times \mathbf{s}\right)}_{\boldsymbol{\pi}'_\beta \in \boldsymbol{\pi}_\beta + I} \bmod \mathbf{B}_J^{pk}$.

- If $b=0$, $\mathbf{t} \leftarrow \mathrm{Samp}_1(R) \bmod \mathbf{B}_J^{pk}$ and $\boldsymbol{\psi}_\beta = \left(\boldsymbol{\pi}_\beta + \mathbf{t} \times \mathbf{s}\right) \bmod \mathbf{B}_J^{pk}$

$$= \underbrace{\left(\boldsymbol{\pi}_\beta + \mathrm{Samp}_1(R) \times \mathbf{s}\right)}_{\boldsymbol{\pi}'_\beta \leftarrow \mathrm{Samp}\left(\boldsymbol{\pi}_\beta,\, \mathbf{B}_I\right)} \bmod \mathbf{B}_J^{pk} = \mathrm{Encrypt}\left(\mathbf{B}_J^{pk}, \boldsymbol{\pi}_\beta\right).$$

$$\Pr[b = b' \mid b = 0] = \Pr[\beta = \beta' \mid b = 0] = 1/2 + \varepsilon.$$

- If $b=1$, $\mathbf{t} \leftarrow_{\text{uniform}} R \bmod \mathbf{B}_J^{pk}$, so $\boldsymbol{\psi}_\beta = \left(\boldsymbol{\pi}_\beta + \mathbf{t} \times \mathbf{s}\right) \bmod \mathbf{B}_J^{pk}$

is unformly random (for $I = (\mathbf{s})$ is relatively prime to $J \Rightarrow$

$\mathbf{s}^{-1}$ exists $\Rightarrow$ $\mathbf{t} \mapsto \boldsymbol{\pi}_\beta + \mathbf{t} \times \mathbf{s}$ bijective $\Rightarrow \boldsymbol{\pi}_\beta + \mathbf{t} \times \mathbf{s}$ uniform.)

$$\Pr[b = b' \mid b = 1] = \Pr[\beta \neq \beta' \mid b = 1] = 1/2.$$

- Thus, B has advantage $\varepsilon/2$.