How Ideal Lattices unlocked Fully Homomorphic Encryption

Francisco José VIAL PRADO

December 10, 2014

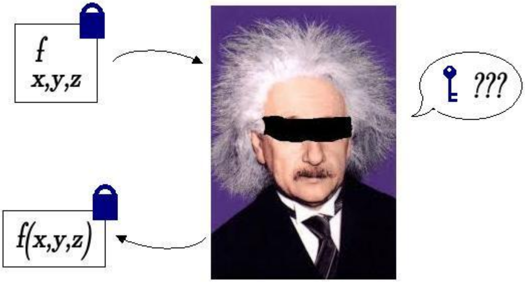
Ph.D. advisor : Louis GOUBIN

This talk

- Introduction
- Gentry's Ideal Lattices scheme
- Further advances, others schemes and open problems

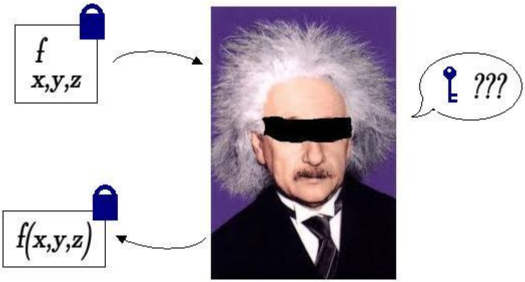
Fully Homomorphic Encryption

Question : "Is it possible to compute blindfolded?"



Fully Homomorphic Encryption

Question : "Is it possible to compute blindfolded?"



Example : A public-key cryptosystem $\mathcal{E}$ verifying : $\forall a, b \in \mathcal{P}(\mathcal{E})$,

$$a + b = \mathrm{D}_{\mathcal{E}}(\mathrm{E}_{\mathcal{E}}(a) + \mathrm{E}_{\mathcal{E}}(b)),$$
$$a \times b = \mathrm{D}_{\mathcal{E}}(\mathrm{E}_{\mathcal{E}}(a) \times \mathrm{E}_{\mathcal{E}}(b)).$$

Formal definition

Def. 1 : A **homomorphic scheme** is a public-key scheme $\mathcal{E}$ with four PPT algorithms :

- KeyGen: $\lambda \mapsto (\mathtt{sk}, \mathtt{pk})$;
- Enc: $(m, \mathtt{pk}) \mapsto c$;
- Dec: $(c, \mathtt{sk}) \mapsto m$;
- Eval:$(C, c_1, \ldots, c_n, \mathtt{pk}) \mapsto m$.

Formal definition

Def. 1 : A **homomorphic scheme** is a public-key scheme $\mathcal{E}$ with four PPT algorithms :

- $\mathtt{KeyGen}$: $\lambda \mapsto (\mathtt{sk}, \mathtt{pk})$;
- $\mathtt{Enc}$: $(m, \mathtt{pk}) \mapsto c$;
- $\mathtt{Dec}$: $(c, \mathtt{sk}) \mapsto m$;
- $\mathtt{Eval}$:$(C, c_1, \ldots, c_n, \mathtt{pk}) \mapsto m$.

Def. 2 : A homomorphic scheme is *correct* for a set of circuits $\mathcal{C}$ if, for every circuit in $\mathcal{C}$,

$$\psi \leftarrow \mathtt{Eval}(C, \psi_1, \ldots, \psi_n, \mathtt{pk}) \;\Rightarrow\; \mathtt{Dec}(\psi, \mathtt{sk}) = C(\pi_1, \ldots, \pi_n)$$

where $\psi_i = \mathtt{Enc}(\pi_i, \mathtt{pk}), i = 1, \ldots, n$.

A **Fully Homomorphic Scheme** is a homomorphic scheme that is correct for all circuits.

Starting point

- Let I be an ideal of some ring R,
- $m \in R$ the message.

Starting point

- Let I be an ideal of some ring R,
- $m \in R$ the message.

Encryption : $\texttt{Enc}(m) = m + xI$ for some $x \in R$.

Search an ideal I that allows

- Random sampling from $\alpha + I, \alpha \in R$.

Search an ideal I that allows

- Random sampling from $\alpha + I, \alpha \in R$.
- Noise annihilation $m + xI \mapsto m$.

Search an ideal I that allows

- Random sampling from $\alpha + I, \alpha \in R$.
- Noise annihilation $m + xI \mapsto m$.

And strong security properties.

Ideals + lattices = Ideal lattices

Let $R = \mathbb{Z}[X]/(X^n + 1)$ where n is a power of 2, and consider the mapping $\alpha : R \to \mathbb{Z}^n$,

$$\alpha(v_0 + v_1 X + \cdots + v_{n-1} X^{n-1}) = (v_0, v_1, \cdots, v_{n-1})$$

Let $I = (P(X))$ be a principal ideal of R :

Ideals + lattices = Ideal lattices

Let $R = \mathbb{Z}[X]/(X^n + 1)$ where n is a power of 2, and consider the mapping $\alpha : R \to \mathbb{Z}^n$,

$$\alpha(v_0 + v_1 X + \cdots + v_{n-1} X^{n-1}) = (v_0, v_1, \cdots, v_{n-1})$$

Let $I = (P(X))$ be a principal ideal of R :

An **ideal lattice** is the image of a principal ideal of R by α, i.e. $L = \alpha(I)$.

Ideals + lattices = Ideal lattices

Let $R = \mathbb{Z}[X]/(X^n + 1)$ where n is a power of 2, and consider the mapping $\alpha : R \to \mathbb{Z}^n$,

$$\alpha(v_0 + v_1 X + \cdots + v_{n-1}X^{n-1}) = (v_0, v_1, \cdots, v_{n-1})$$

Let $I = (P(X))$ be a principal ideal of R :

An **ideal lattice** is the image of a principal ideal of R by α, i.e. $L = \alpha(I)$.

For instance, if $n = 3$, $\alpha((2 + X))$ is generated by

$$\langle \alpha(2 + X), \alpha(X(2 + X)), \alpha(X^2(2 + X)) \rangle.$$

Ideals + lattices = Ideal lattices

Let $R = \mathbb{Z}[X]/(X^n + 1)$ where n is a power of 2, and consider the mapping $\alpha : R \to \mathbb{Z}^n$,

$$\alpha(v_0 + v_1 X + \cdots + v_{n-1} X^{n-1}) = (v_0, v_1, \cdots, v_{n-1})$$

Let $I = (P(X))$ be a principal ideal of R :

An **ideal lattice** is the image of a principal ideal of R by α, i.e. $L = \alpha(I)$.

For instance, if $n = 3$, $\alpha((2 + X))$ is generated by

$$\langle \alpha(2 + X), \alpha(X(2 + X)), \alpha(X^2(2 + X)) \rangle.$$

I.e., the columns of $\begin{pmatrix} 2 & 0 & -1 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$.

Operations in an ideal lattice

Let L be an ideal lattice with base $\mathbf{B}_L = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Define

$$P(\mathbf{B}_L) = \left\{ \sum_{i \leq n} x_i \mathbf{b}_i \in \mathbb{R}^n \ ; \ x_i \in [-1/2, 1/2) \right\}.$$

Operations in an ideal lattice

Let L be an ideal lattice with base $\mathbf{B}_L = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Define

$$P(\mathbf{B}_L) = \left\{ \sum_{i \leq n} x_i \mathbf{b}_i \in \mathbb{R}^n \ ; \ x_i \in [-1/2, 1/2) \right\}.$$

- Base reduction in $\mathbb{Z}^n$: $x \bmod \mathbf{B}_L = x - \mathbf{B}_L \lfloor \mathbf{B}_L^{-1} x \rceil \in \mathcal{P}(\mathbf{B}_L)$

Operations in an ideal lattice

Let L be an ideal lattice with base $\mathbf{B}_L = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Define

$$P(\mathbf{B}_L) = \left\{ \sum_{i \leq n} x_i \mathbf{b}_i \in \mathbb{R}^n \; ; \; x_i \in [-1/2, 1/2) \right\}.$$

- Base reduction in $\mathbb{Z}^n$: $x \bmod \mathbf{B}_L = x - \mathbf{B}_L \lfloor \mathbf{B}_L^{-1} x \rceil \in \mathcal{P}(\mathbf{B}_L)$
- Addition in $\mathbb{Z}^n$: $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} + \mathbf{y}$

Operations in an ideal lattice

Let L be an ideal lattice with base $\mathbf{B}_L = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Define

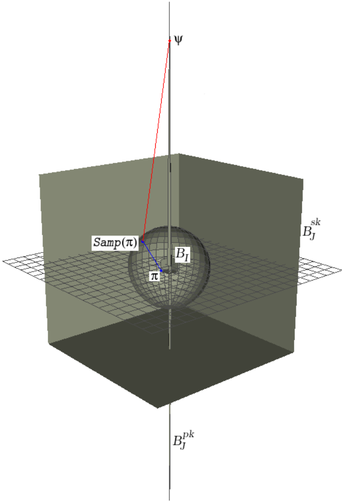
$$P(\mathbf{B}_L) = \left\{ \sum_{i \le n} x_i \mathbf{b}_i \in \mathbb{R}^n \; ; \; x_i \in [-1/2, 1/2) \right\}.$$

- Base reduction in $\mathbb{Z}^n$: $x \bmod \mathbf{B}_L = x - \mathbf{B}_L \lfloor \mathbf{B}_L^{-1} x \rceil \in \mathcal{P}(\mathbf{B}_L)$
- Addition in $\mathbb{Z}^n$: $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} + \mathbf{y}$
- Product in $\mathbb{Z}^n$: $(\mathbf{x}, \mathbf{y}) \mapsto \alpha(\mathbf{x}(X) \times \mathbf{y}(X))$

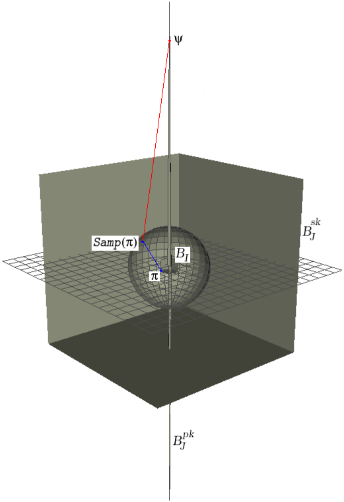
Gentry's solution

- Let J be an ideal lattice, generated by two bases $\mathbf{B}_J^{\mathrm{sk}}, \mathbf{B}_J^{\mathrm{pk}}$.
- $\mathcal{P} \subseteq \{0,1\}^n$, $\mathtt{pk} = \{\mathbf{B}_J^{\mathrm{pk}}\}$, $\mathtt{sk} = \{\mathbf{B}_J^{\mathrm{sk}}\}$
- Let $\mathtt{Samp}(\pi)$ be a (bounded) random algorithm that samples from $\pi + 2\mathbb{Z}^n$.

Gentry's solution



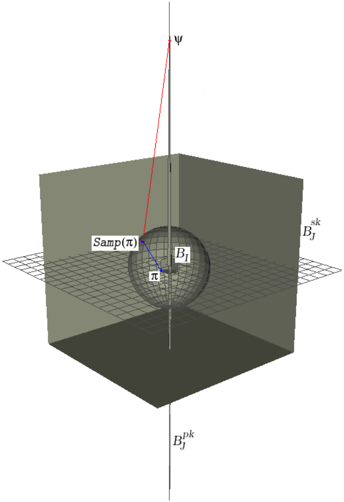
Gentry's solution



Encryption :

$$\vec{\pi} \xrightarrow{\texttt{Samp}} \vec{\pi}+2\vec{e}$$

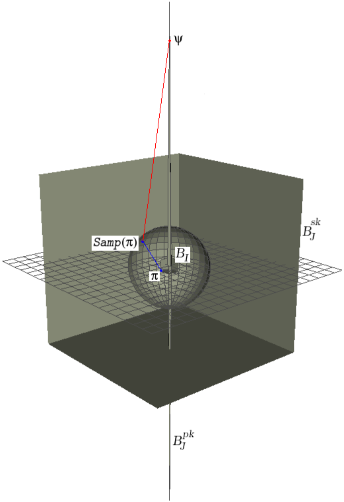
Gentry's solution



Encryption :

$$\vec{\pi} \xrightarrow{\texttt{Samp}} \vec{\pi}+2\vec{e} \xrightarrow{\text{mod } \mathbf{B}_J^{\texttt{pk}}} \vec{\pi}+2\vec{e}+\vec{i}.$$

Gentry's solution



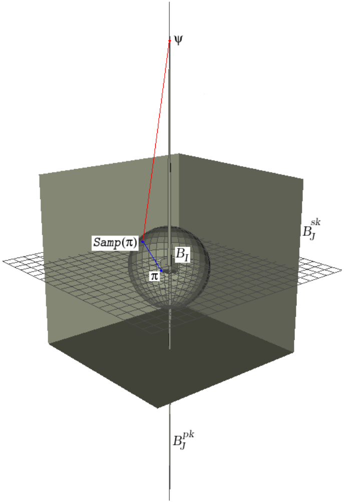
Encryption :

$$\vec{\pi} \xrightarrow{\texttt{Samp}} \vec{\pi}+2\vec{e} \xrightarrow{\text{mod } \mathbf{B}_J^{\texttt{pk}}} \vec{\pi}+2\vec{e}+\vec{i}.$$

Decryption :

$$\vec{\psi} \xrightarrow{\text{mod } \mathbf{B}_J^{\texttt{sk}}} \vec{\psi}-\vec{i}'$$

Gentry's solution



Encryption :

$$\vec{\pi} \xrightarrow{\texttt{Samp}} \vec{\pi}+2\vec{e} \xrightarrow{\text{mod } \mathbf{B}_J^{\texttt{pk}}} \vec{\pi}+2\vec{e}+\vec{i}.$$

Decryption :

$$\vec{\psi} \xrightarrow{\text{mod } \mathbf{B}_J^{\texttt{sk}}} \vec{\psi}-\vec{i'} \xrightarrow{\text{mod } 2} \vec{\pi}-\vec{i'}-\vec{2e'}.$$

Homomorphic properties

$$\psi = \vec{\pi} + 2\vec{e} + i, \ \psi' = \vec{\pi}' + 2\vec{e}' + i'$$

Homomorphic properties

$$\psi = \vec{\pi} + 2\vec{e} + i, \ \psi' = \vec{\pi}' + 2\vec{e}' + i'$$

$$\psi + \psi' = (\vec{\pi} + \pi') + 2(\vec{e} + \vec{e}') + i''$$

$$\psi \times \psi' = (\vec{\pi} \times \pi') + 4\vec{e} \times \vec{e}' + i'''$$

Homomorphic properties

$$\psi = \vec{\pi} + 2\vec{e} + i, \ \psi' = \vec{\pi}' + 2\vec{e}' + i'$$

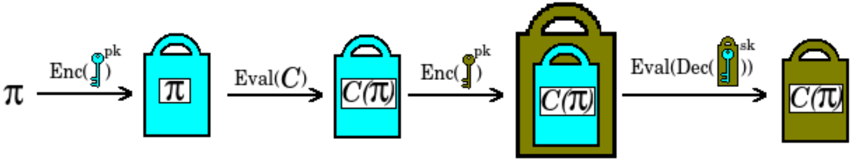
$$\psi + \psi' = (\vec{\pi} + \pi') + 2(\vec{e} + \vec{e}') + i''$$

$$\psi \times \psi' = (\vec{\pi} \times \pi') + 4\vec{e} \times \vec{e}' + i'''$$

Theorem : $d_{\max} = \log\log ||\vec{v}_{\mathtt{sk}}||_2 - \log\log(\sqrt{n} \cdot l_{\mathtt{Samp}})$

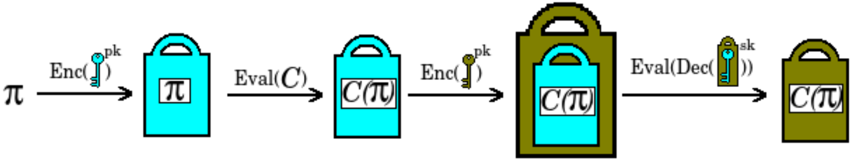
Ground-breaking idea

Bootstrapping : Capability of refreshing a high-noise message.



Ground-breaking idea

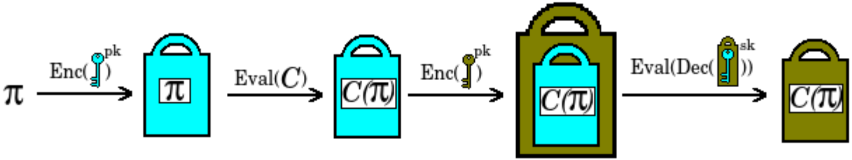
Bootstrapping : Capability of refreshing a high-noise message.



- The scheme has to verify : $D_{\mathcal{E}} \in C_{\mathcal{E}}$.

Ground-breaking idea

Bootstrapping : Capability of refreshing a high-noise message.



- The scheme has to verify : $D_{\mathcal{E}} \in C_{\mathcal{E}}$.
- Introduces "circular security" issues.

Bootstrapping theorem : Let $\mathcal{E}$ be a homomorphic encryption scheme that is correct for circuits in $\mathcal{C}$. If $\mathtt{Dec}_{\mathcal{E}} \in \mathcal{C}$, then $\mathcal{E}$ is bootstrappable.

Bootstrapping theorem : Let $\mathcal{E}$ be a homomorphic encryption scheme that is correct for circuits in $\mathcal{C}$. If $\mathtt{Dec}_{\mathcal{E}} \in \mathcal{C}$, then $\mathcal{E}$ is bootstrappable.

For reasonable parameters, the I.L. scheme as presented is **not** bootstrappable.

Bootstrapping theorem : Let $\mathcal{E}$ be a homomorphic encryption scheme that is correct for circuits in $\mathcal{C}$. If $\texttt{Dec}_{\mathcal{E}} \in \mathcal{C}$, then $\mathcal{E}$ is bootstrappable.

For reasonable parameters, the I.L. scheme as presented is **not** bootstrappable.

Gentry reduces the degree of the decryption circuit and achieves bootstrapping.

New security issues

Circular security : Is it safe to send Key-Dependent messages ? If so; is this provable ?

New security issues

Circular security : Is it safe to send Key-Dependent messages ? If so; is this provable ?

The Sparse Subset Sum Vector Problem : Given an upper bound for θ, distinguish between

$$\{\vec{t}_1, \ldots, \vec{t}_\Theta\} \subset^R \mathbb{Q}^n \text{ and } \{\vec{t}_1, \ldots, \vec{t}_\Theta \in \mathbb{Q}^n; \sum_{i \in S} \vec{t}_i = 0\}.$$

Other FHE schemes

van Dijk, Gentry, Halevi, Vaikuntanathan.– A FHE scheme over $\mathbb{Z}$.

Brakerski, Vaikuntanathan.— (i) FHE from LWE (ii) FHE with proved circular security

Multikey FHE

- Ciphertexts are to be decrypted jointly by a set of secret-key holders
- Allows Multiparty Computation Protocols in the cloud

Multikey FHE

- Ciphertexts are to be decrypted jointly by a set of secret-key holders
- Allows Multiparty Computation Protocols in the cloud

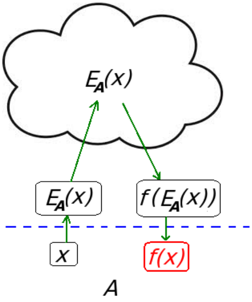
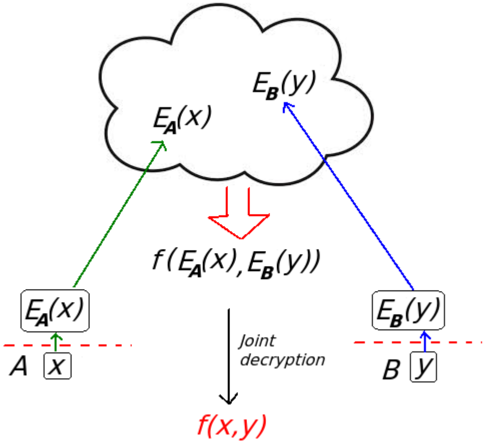
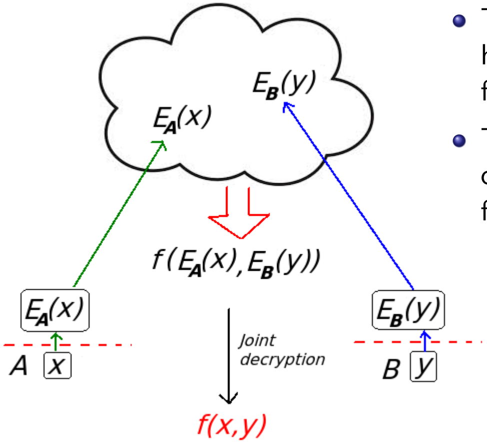


Figure : Single Key FHE scenario

MPC on the cloud



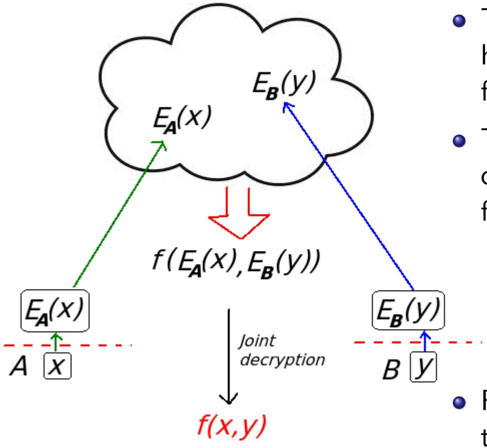
MPC on the cloud



- The cloud computes the homomorphic evaluation as for in the single key setting.
- The decryption is the joint computation of the function

$$\mathtt{Dec}(C, \mathtt{sk}_A, \mathtt{sk}_B).$$

MPC on the cloud



- The cloud computes the homomorphic evaluation as for in the single key setting.
- The decryption is the joint computation of the function

$$\mathtt{Dec}(C, \mathtt{sk}_A, \mathtt{sk}_B).$$

- Reduction of general MPC to a particular MPC !

Attribute-Based and Identity-Based FHE scheme

2013 : The *approximate eigenvector problem* :

Attribute-Based and Identity-Based FHE scheme

2013 : The *approximate eigenvector problem* :

$$C\,\vec{v} = \mu\,\vec{v} + \vec{e}$$

- Ciphertexts are matrices
- Security comes from LWE
- Assymptotically faster

Attribute-Based and Identity-Based FHE scheme

2013 : The *approximate eigenvector problem* :

$$C\,\vec{v} = \mu\,\vec{v} + \vec{e}$$

- Ciphertexts are matrices
- Security comes from LWE
- Assymptotically faster
- They provide a compiler to convert any LWE-FHE scheme into an attribute based scheme

Attribute-Based and Identity-Based FHE scheme

2013 : The *approximate eigenvector problem* :

$$C\,\vec{v} = \mu\,\vec{v} + \vec{e}$$

- Ciphertexts are matrices
- Security comes from LWE
- Assyptotically faster
- They provide a compiler to convert any LWE-FHE scheme into an attribute based scheme
- or into a (hierarchical) identity based scheme.

Hierarchical encryption

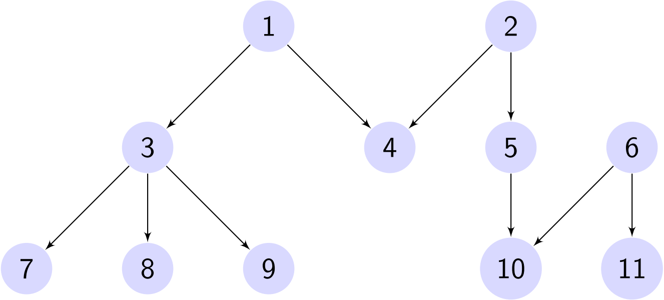


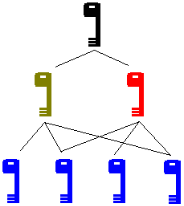
Figure : A polytree.

Hierarchical encryption

- A high level user can "merge" all subordinate keys into a single one

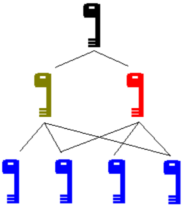
Hierarchical encryption

- A high level user can "merge" all subordinate keys into a single one



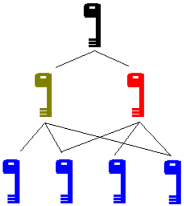
Hierarchical encryption

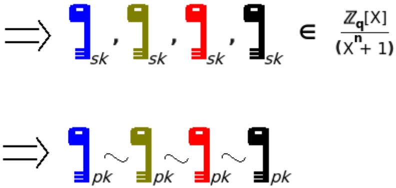
- A high level user can "merge" all subordinate keys into a single one



Hierarchical encryption

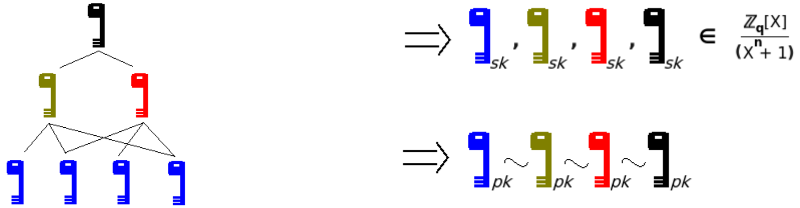
- A high level user can "merge" all subordinate keys into a single one





Hierarchical encryption

- A high level user can "merge" all subordinate keys into a single one



- Changes can be done in the tree in real time
- Two distant users can collaborate regardless of the authority level

(Work in progress...)

Open questions

Open questions

- FHE + equality test ?

Open questions

- FHE + equality test ?
- "Targeted" FHE: allow only a class of public computations.

Open questions

- FHE + equality test ?
- "Targeted" FHE: allow only a class of public computations.
- Is it possible to exploit the "graph structure" on ciphertexts via $C + E(0)$ or $C \times E(1)$?

Thank you!