
Group Action Systems:
a Mathematical tool for deriving
Provable Secure Cryptographic Schemes

María Isabel González Vasco



Group Action Systems: a Mathematical tool for deriving Provable Secure Cryptographic Schemes

Joint works with J. L. Villar (UPC) and R. Steinwandt (FAU)

Overview

- Introduction



Overview

- Introduction
- Some basics about PHFs
 - Definitions
 - Basic Results
 - Cryptographic Applications



Overview



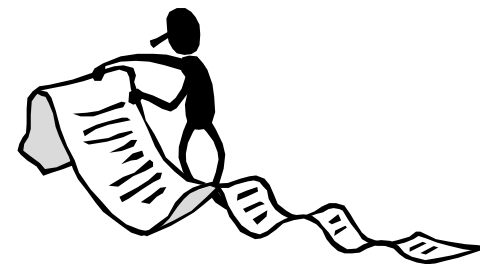
- Introduction
- Some basics about PHFs
 - Definitions
 - Basic Results
 - Cryptographic Applications
- Group Action Based PHFs
 - Group Action Systems
 - Useful AcPHFs. Diversity.

Overview



- Introduction
- Some basics about PHFs
 - Definitions
 - Basic Results
 - Cryptographic Applications
- Group Action Based PHFs
 - Group Action Systems
 - Useful AcPHFs. Diversity.
- Examples

Overview



- Introduction
- Some basics about PHFs
 - Definitions
 - Basic Results
 - Cryptographic Applications
- Group Action Based PHFs
 - Group Action Systems
 - Useful AcPHFs. Diversity
- Examples
- Final Remarks

Introduction

- Motivation: finding new suitable mathematical primitives for cryptographic designs.

Introduction

- Motivation: finding new suitable mathematical primitives for cryptographic designs.
- Fact: work in that direction hardly exploits the constructions and theoretical frameworks available from number-theoretical cryptography.

Introduction

- Motivation: finding new suitable mathematical primitives for cryptographic designs.
- Fact: work in that direction hardly exploits the constructions and theoretical frameworks available from number-theoretical cryptography.
- Our Goal: adapt the existing theory of Universal Projective Hash Functions to allow constructions arising in different areas of mathematics .

Some basics about PHFs

Definitions

Let X, Π, S be non-empty sets, $L \subseteq X$, and K a finite index set.

Consider $H := \{ H_k : X \mapsto \Pi \}_{k \in K}$ and $\alpha : K \mapsto S$.

Definitions

Let X, Π, S be non-empty sets, $L \subseteq X$, and K a finite index set.

Consider $H := \{ H_k : X \mapsto \Pi \}_{k \in K}$ and $\alpha : K \mapsto S$.

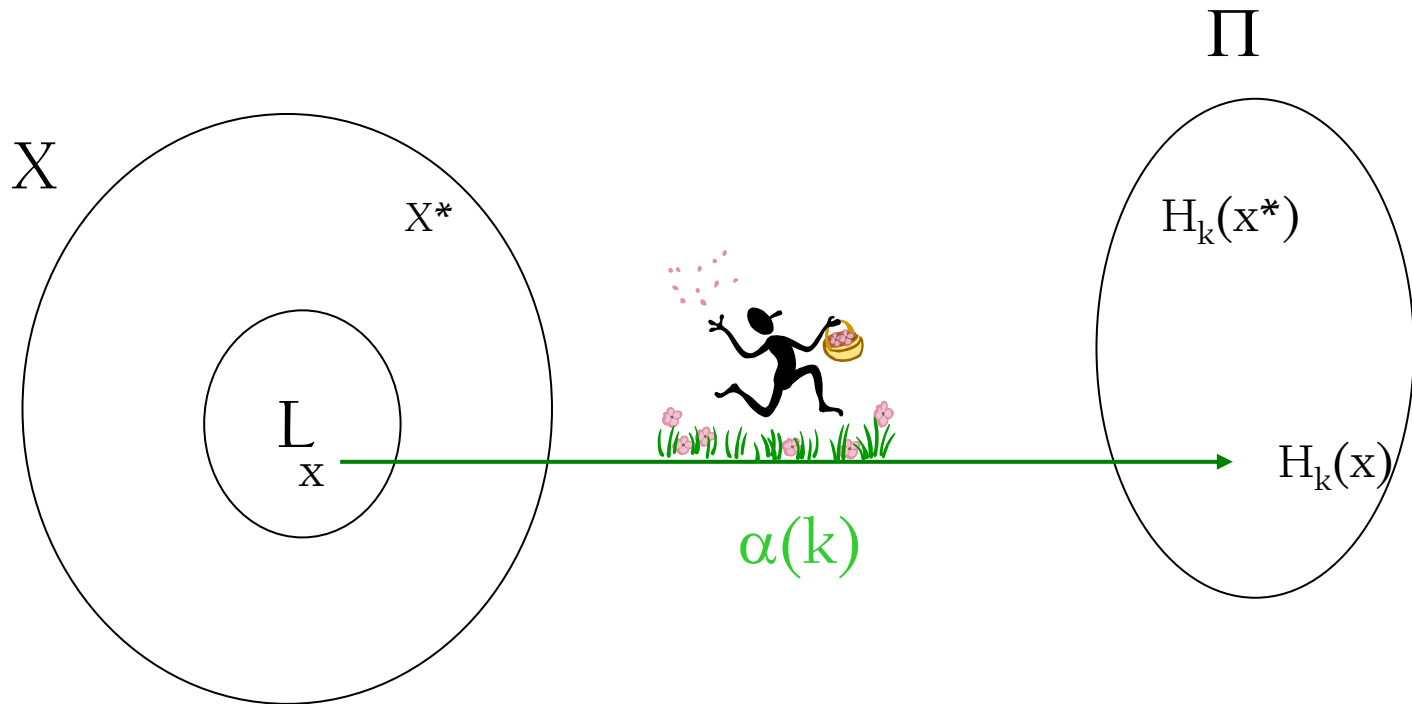
Then the tuple $H = (H, K, X, L, \Pi, S, \alpha)$ is a *projective hash family*

- PHF - for (X, L) provided that

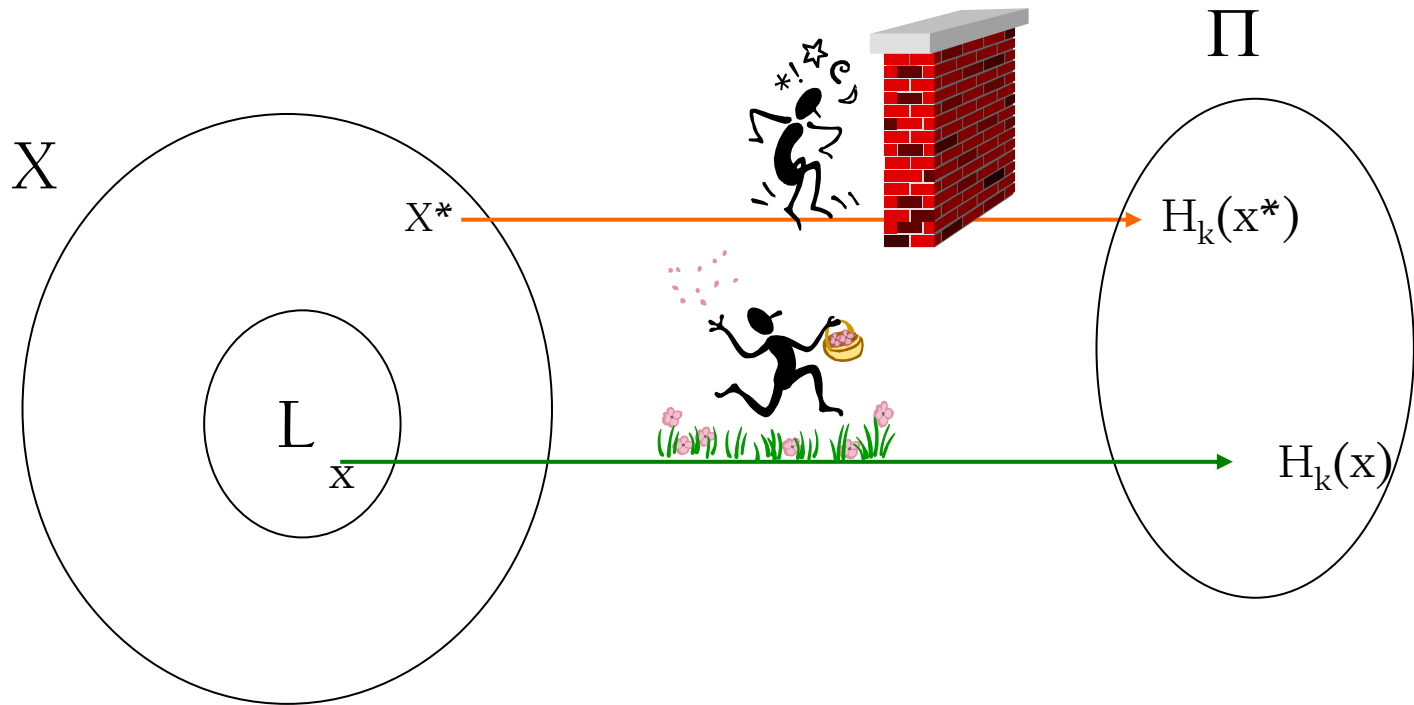
$$\alpha(k) \approx H_{k|L}()$$

(i.e., $\forall x \in L, k_1, k_2 \in K, \alpha(k_1) = \alpha(k_2) \Rightarrow H_{k_1}(x) = H_{k_2}(x)$).

Given only the projection $\alpha(k)$...



...it could be hard to compute H_k outside L



Definitions

Moreover, we say that $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$ is

→ ε -universal $:\Leftrightarrow \forall s \in S, x \in X \setminus L, \pi \in \Pi$
 $P[H_k(x) = \pi / \alpha(k)=s] \leq \varepsilon;$

Definitions

Moreover, we say that $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$ is

→ ε -universal $:\Leftrightarrow \forall s \in S, x \in X \setminus L, \pi \in \Pi$

$$P[H_k(x) = \pi / \alpha(k)=s] \leq \varepsilon;$$

→ ε -universal₂ $:\Leftrightarrow \forall s \in S, x \in X \setminus L, x^* \in X \setminus (L \cup \{x\}), \pi, \pi^* \in \Pi$

$$P[H_k(x) = \pi / H_k(x^*) = \pi^*, \alpha(k)=s] \leq \varepsilon;$$

Definitions

Moreover, we say that $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$ is

→ ε -universal $:\Leftrightarrow \forall s \in S, x \in X \setminus L, \pi \in \Pi$

$$P[H_k(x) = \pi / \alpha(k) = s] \leq \varepsilon;$$

→ ε -universal₂ $:\Leftrightarrow \forall s \in S, x \in X \setminus L, x^* \in X \setminus (L \cup \{x\}), \pi, \pi^* \in \Pi$

$$P[H_k(x) = \pi / H_k(x^*) = \pi^*, \alpha(k) = s] \leq \varepsilon;$$

→ ε -smooth $:\Leftrightarrow (x, \alpha(k), H_k(x))$ and $(x, \alpha(k), \pi)$ are ε -close for $k \in K, x \in X \setminus L$ and $\pi \in \Pi$ chosen uniformly at random ;

Definitions

Moreover, we say that $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$ is

→ ε -universal $:\Leftrightarrow \forall s \in S, x \in X \setminus L, \pi \in \Pi$

$$P[H_k(x) = \pi / \alpha(k) = s] \leq \varepsilon;$$

→ ε -universal₂ $:\Leftrightarrow \forall s \in S, x \in X \setminus L, x^* \in X \setminus (L \cup \{x\}), \pi, \pi^* \in \Pi$

$$P[H_k(x) = \pi / H_k(x^*) = \pi^*, \alpha(k) = s] \leq \varepsilon;$$

→ ε -smooth $:\Leftrightarrow (x, \alpha(k), H_k(x))$ and $(x, \alpha(k), \pi)$ are ε -close for $k \in K, x \in X \setminus L$ and $\pi \in \Pi$ chosen uniformly at random;

→ Strongly universal₂ \approx worst case smoothness.

Basic Results

- Ways of “upgrading” the weaker types of PHFs to achieve more robust types:
 - Universal to universal_2 - Cramer and Shoup, [EUROCRYPT 2002]
 - Universal to smooth - Cramer and Shoup, [EUROCRYPT 2002]
 - Universal_2 to strongly universal_2

Basic Results

- Ways of “upgrading” the weaker types of PHFs to achieve more robust types:
 - Universal to universal₂ - Cramer and Shoup, [EUROCRYPT 2002]
 - Universal to smooth - Cramer and Shoup, [EUROCRYPT 2002]
 - Universal₂ to strongly universal₂
- Methods for constructing cryptographically useful PHFs

Cryptographic Applications

- Cramer and Shoup [EUROCRYPT 2002]
 - IND-CCA Encryption Scheme in the standard model

Cryptographic Applications

- Cramer and Shoup [EUROCRYPT 2002]
 - IND-CCA Encryption Scheme in the standard model
- Kurosawa and Desmedt [CRYPTO 2004]
 - Hybrid encryption scheme

Cryptographic Applications

- Cramer and Shoup [EUROCRYPT 2002]
 - IND-CCA Encryption Scheme in the standard model
- Kurosawa and Desmedt [CRYPTO 2004]
 - Hybrid encryption scheme
- Genaro and Lindell [EUROCRYPT 2003]
 - Password based authenticated key exchange

Cryptographic Applications

- Cramer and Shoup [EUROCRYPT 2002]
 - IND-CCA Encryption Scheme in the standard model
- Kurosawa and Desmedt [CRYPTO 2004]
 - Hybrid encryption scheme
- Genaro and Lindell [EUROCRYPT 2003]
 - Password based authenticated key exchange
- Kalai [EUROCRYPT 2005]
 - 2-out-of-1 oblivious transfer protocol.

Cryptographic Applications

- Cramer and Shoup [EUROCRYPT 2002]
 - Π is the message space
 - k is kept secret, $\alpha(k)$ and x are public
 - $m \in \Pi$ is encrypted using $H_k(x)$ as a one time pad, for $x \in L$, i.e.,
$$E(\alpha(k))(m) = (x, H_k(x) \oplus m)$$
 - IND-CCA security is achieved by appending a proof of integrity

Cryptographic Applications

■ Kalai [EUROCRYPT 2005]

Sender's (B) input: two strings γ_0, γ_1 ,

Receiver's (A) input: choice bit b .

Goal: A learns γ_b , but nothing about γ_{b-1} . B learns nothing about b .

Cryptographic Applications

■ Kalai [EUROCRYPT 2005]

Sender's (B) input: two strings γ_0, γ_1 .

Receiver's (A) input: choice bit b .

Goal: A learns γ_b , but nothing about γ_{1-b} . B learns nothing about b .

- A chooses $x_b \in L$ and $x_{1-b} \in X \setminus L$ and sends (X, x_0, x_1) to B;

Cryptographic Applications

■ Kalai [EUROCRYPT 2005]

Sender's (B) input: two strings γ_0, γ_1 .

Receiver's (A) input: choice bit b .

Goal: A learns γ_b , but nothing about γ_{1-b} . B learns nothing about b .

- A chooses $x_b \in L$ and $x_{1-b} \in X \setminus L$ and sends (X, x_0, x_1) to B;
- B chooses independently two random keys k_0, k_1 and sends $\alpha(k_0), \alpha(k_1), y_0 = \gamma_0 \oplus H_{k_0}(x_0)$ and $y_1 = \gamma_1 \oplus H_{k_1}(x_1)$;

Cryptographic Applications

■ Kalai [EUROCRYPT 2005]

Sender's (B) input: two strings γ_0, γ_1 .

Receiver's (A) input: choice bit b .

Goal: A learns γ_b , but nothing about γ_{1-b} . B learns nothing about b .

- A chooses $x_b \in L$ and $x_{1-b} \in X \setminus L$ and sends (X, x_0, x_1) to B;
- B chooses independently two random keys k_0, k_1 and sends $\alpha(k_0), \alpha(k_1), y_0 = \gamma_0 \oplus H_{k_0}(x_0)$ and $y_1 = \gamma_1 \oplus H_{k_1}(x_1)$;
- A retrieves γ_b by computing $y_b \oplus H_{k_b}(x_b)$ using the projection key $\alpha(k_b)$. Note that as $x_{1-b} \in X \setminus L$, $\alpha(k_{1-b})$ does not give enough information for computing $H_{k_{1-b}}$ outside L .

Group Action Based Projective Hash Families

Group Systems

- “Atoms” from which PHFs are derived for Cramer-Shoup Encryption Scheme [EUROCRYPT 2002].

Group Systems

- “Atoms” from which PHFs are derived for Cramer-Shoup Encryption Scheme [EUROCRYPT 2002].
- A *group system* is a tuple (H, X, L, Π) , where X and Π are finite abelian groups, $L \leq X$, $H \leq \text{Hom}(X, \Pi)$.

Group Systems

- “Atoms” from which PHFs are derived for Cramer-Shoup Encryption Scheme [EUROCRYPT 2002].
- A *group system* is a tuple (H, X, L, Π) , where X and Π are finite abelian groups, $L \leq X$, $H \leq \text{Hom}(X, \Pi)$.
- To derive a PHF, one must specify the action of H on L in terms of a set $\{g_1, \dots, g_d\}$ of generators for L , i.e.

$$\alpha(k) = (H_k(g_1), \dots, H_k(g_d)).$$

Group Systems

- “Atoms” from which PHFs are derived for Cramer and Shoup’s Encryption Scheme [EUROCRYPT 2002].
- A *group system* is a tuple (H, X, L, Π) , where X and Π are finite abelian groups, $L \leq X$, $H \leq \text{Hom}(X, \Pi)$.
- To derive a PHF, one must specify the action of H on L in terms of a set $\{g_1, \dots, g_l\}$ of generators for L , i.e.
$$\alpha(k) = (H_k(g_1), \dots, H_k(g_l)).$$
- Using group systems, they derived instances of their encryption scheme based on the DDH problem and the Decision Composite Residuosity assumption.

Group Action Systems (I)

Let X be a finite set and H a finite group left-acting on X . Denote by $\phi(h)$ the permutation induced by $h \in H$ on X .

Group Action Systems (I)

Let X be a finite set and H a finite group left-acting on X . Denote by $\phi(h)$ the permutation induced by $h \in H$ on X .

Let S be a finite group and $\chi: H \mapsto S$ a group homomorphism.

Then, the tuple (X, H, χ, S) is called a *group action system*.

Group Action Systems (II)

Given a group action system (X, H, χ, S) , a PHF can be constructed via a suitable indexing of H , i.e., given a finite set K , $\tilde{h} : K \mapsto H$ the tuple

$(X, H, K, S, \chi, \tilde{h})$ defines a PHF (AcPHF)

$$H = (H, K, X, L, X, S, \chi \circ \tilde{h}),$$

where

$$L := \{ x \in X \mid |(\text{Ker}\chi)(x)| = 1 \}.$$

Group Action Systems (III)

Note that:

- $L := \{ x \in X \mid (\text{Ker}\chi)(x) = x \};$

Group Action Systems (III)

Note that:

- $L := \{ x \in X \mid (\text{Ker}\chi)(x) = x \};$
- $\text{Ker}\chi \subseteq \text{Stab}(L);$

Group Action Systems (III)

Note that:

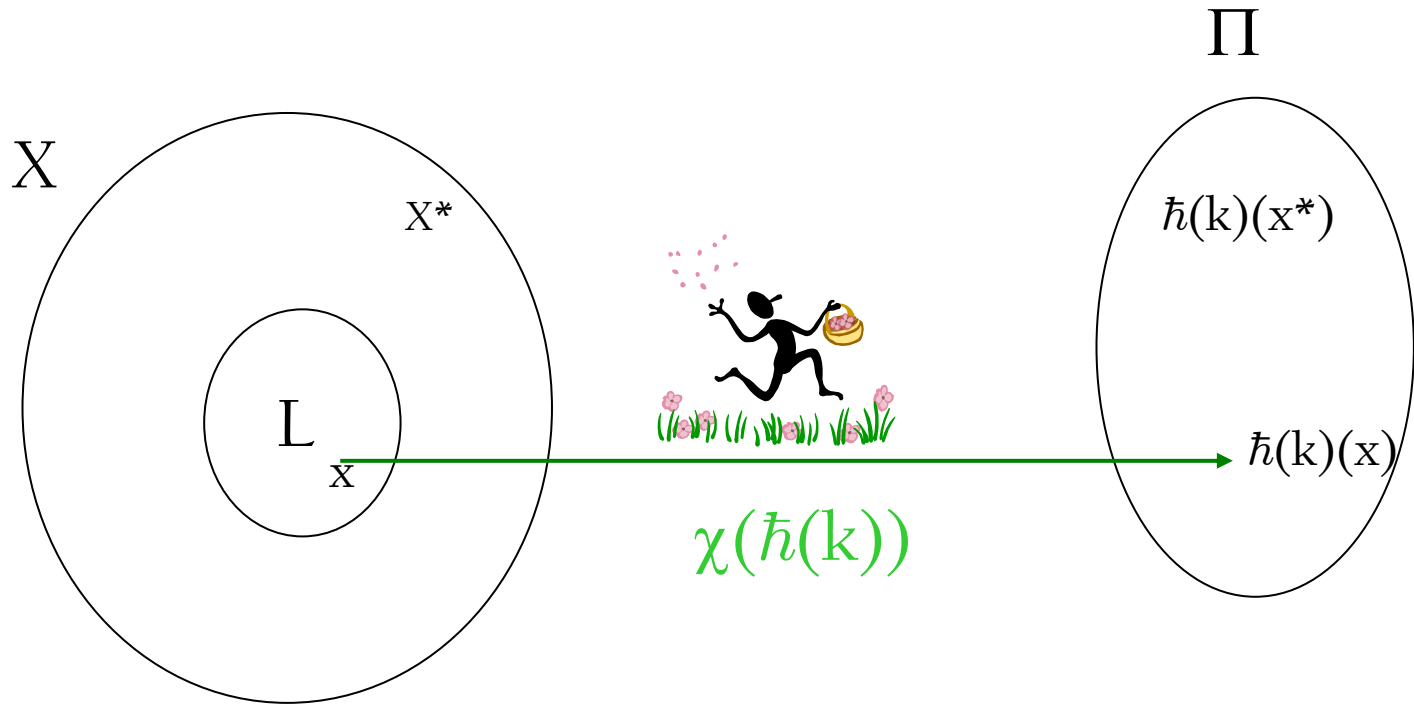
- $L := \{ x \in X \mid (\text{Ker}\chi)(x) = x \}$;
- $\text{Ker}\chi \subseteq \text{Stab}(L)$;
- H leaves L invariant;

Group Action Systems (III)

Note that:

- $L := \{ x \in X \mid (\text{Ker}\chi)(x) = x \}$;
- $\text{Ker}\chi \subseteq \text{Stab}(L)$;
- H leaves L invariant;
- We will be interested in systems for which the $(\text{Ker}\chi)$ -orbits of elements in $X \setminus L$ are large.

ACPHFs



Group Action Based PHFs

Useful ACPHFs.

A group action system (X, H, χ, S) is *p-diverse* if
 $|(\text{Ker}\chi)(\mathbf{x})| \geq p, \forall \mathbf{x} \in X \setminus L.$

Useful ACPHFs.

A group action system (X, H, χ, S) is *p-diverse* if

$$|(\text{Ker}\chi)(\mathbf{x})| \geq p, \quad \forall \mathbf{x} \in X \setminus L.$$

Lemma. If (X, H, χ, S) is *p-diverse*, then $(X, H, K, S, \chi, \hbar)$ is $(1/p)$ -universal.

Useful ACPHFs.

A group action system (X, H, χ, S) is *p-diverse* if

$$|(\text{Ker}\chi)(\mathbf{x})| \geq p, \quad \forall \mathbf{x} \in X \setminus L.$$

Lemma. If (X, H, χ, S) is *p-diverse*, then $(X, H, K, S, \chi, \hbar)$ is $(1/p)$ -universal.

Moreover...

Useful ACPHFs.

A group action system (X, H, χ, S) is *p-diverse* if

$$|(\text{Ker}\chi)(\mathbf{x})| \geq p, \quad \forall \mathbf{x} \in X \setminus L.$$

Lemma. If (X, H, χ, S) is *p-diverse*, then $(X, H, K, S, \chi, \hbar)$ is $(1/p)$ -universal.

Moreover...

...there's a “dedicated” way of upgrading it
to $(1/p)$ -universal₂ !!



Group Action Based PHFs

Examples

An example using linear groups

Let X be F_q^n , $\{\alpha_1, \dots, \alpha_n\}$ and F_q basis for X .

An example using linear groups

Let X be F_q^n , $\{\alpha_1, \dots, \alpha_n\}$ and F_q basis for X .

Let $H \leq GL(n, q)$, leaving a d -dimensional space L invariant.

An example using linear groups

Let X be F_q^n , $\{\alpha_1, \dots, \alpha_n\}$ and F_q basis for X .

Let $H \leq GL(n, q)$, leaving a d -dimensional space L invariant.

Define $\chi : H \mapsto GL(d, q)$

$$M \mapsto M_d$$

An example using linear groups

Let X be F_q^n , $\{\alpha_1, \dots, \alpha_n\}$ and F_q basis for X .

Let $H \leq GL(n, q)$, leaving a d -dimensional space L invariant.

Define $\chi : H \mapsto GL(d, q)$

$$M \mapsto M_d$$

...How to achieve p -diversity?



Examples

An example using non-abelian groups

Take X non-abelian, $H \leq \text{Aut}(X)$,

An example using non-abelian groups

Take X non-abelian, $H \leq \text{Aut}(X)$,

$L \leq X$, H -invariant ($h(L) = L \forall h \in H$)

An example using non-abelian groups

Take X non-abelian, $H \leq \text{Aut}(X)$,

$L \leq X$, H -invariant ($h(L) = L \forall h \in H$)

Construct a projection $\chi: H \mapsto H|_L$ by means of a “group base” of L ; i.e., a sequence $[\alpha_1, \dots, \alpha_n]$, with each $\alpha_i = (\alpha_{i1}, \dots, \alpha_{ir_i})$, $\alpha_{ij_i} \in G$, so that each $g \in L$ can be expressed as a product:

$$g = \alpha_{1j_1} \cdots \alpha_{sj_s}, \text{ where } \alpha_{ij_i} \in \alpha_i.$$

An example using non-abelian groups

Take X non-abelian, $H \leq \text{Aut}(X)$,

$L \leq X$, H -invariant ($h(L) = L \ \forall h \in H$)

Construct a projection $\chi: H \mapsto H|_L$ by means of a “group base” of L ; that is, a sequence $[\alpha_1, \dots, \alpha_n]$, with each $\alpha_i = (\alpha_{i1}, \dots, \alpha_{ir_i})$, $\alpha_{ij_i} \in G$ so that each $g \in L$ can be expressed as a product:

$$g = \alpha_{1j_1} \cdots \alpha_{sj_s}, \text{ where } \alpha_{ij_i} \in \alpha_i .$$

Then,

$$\begin{aligned} \chi : H &\mapsto H|_L \\ h &\mapsto (h(\alpha_{1j_1}), \dots, h(\alpha_{sj_s})) \end{aligned}$$

An example using non-abelian groups

Seems simple but...

Examples

An example using non-abelian groups

Seems simple but...

further requirements are needed!



An example using non-abelian groups (II)

Seems simple but...

further requirements are needed!

For instance, for realising Cramer and Shoup's scheme:

- random elements from L must be hard to distinguish from random elements from X .
- “factoring” $x \in L$ with respect to the group base α should be hard (without trapdoor information)

(for details, see G-V, Martínez, Steinwandt, Villar [TCC 05])

A Geometric Example

Let p be a finite projective plane over a prime field F_q , let X be the point-set of p , L a fixed line in p , and c a fixed point on L .

A Geometric Example

Let p be a finite projective plane over a prime field F_q , let X be the point-set of p , L a fixed line in p , and c a fixed point on L .

Take H the group of elations with center c (note that every elation induces a permutation in the L points).

A Geometric Example

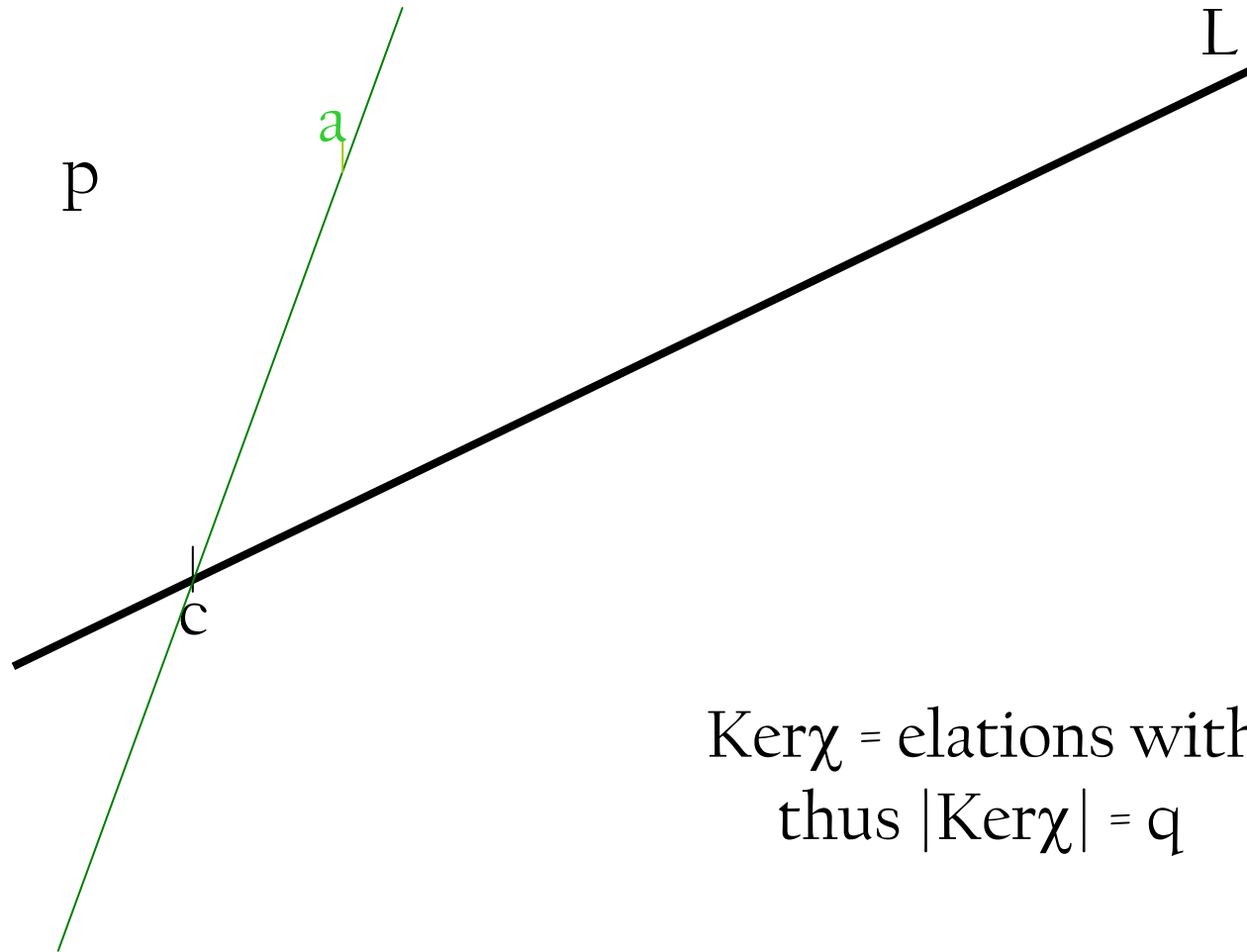
Let p be a finite projective plane over a prime field F_q , let X be the point-set of p , L a fixed line in p , and c a fixed point on L .

Take H the group of elations with center c (note that every elation induces a permutation in the L points).

Define χ as the group homomorphism

$$\begin{aligned}\chi : H &\mapsto S_L \\ \zeta &\mapsto \zeta|_L\end{aligned}$$

A Geometric Example



$\text{Ker}\chi = \text{relations with axis } L,$
thus $|\text{Ker}\chi| = q$

Final Remarks

Final Remarks

- Given a suitable group action system, we know how to construct “good” PHFs.

Final Remarks

- Given a suitable group action system, we know how to construct “good” PHFs.
- Unfortunately, so far “good” \neq “good enough”, as the main cryptographic constructions require additional properties.



Final Remarks

Final Remarks

- Given a suitable group action system, we know how to construct “good” PHFs.
- Unfortunately, so far “good” \neq “good enough”, as the main cryptographic constructions require additional properties.
- However, this framework sheds some light on how to use (robust enough) problems not yet exploited.

Thank you!!!
