

**Towards
Provably Secure Asymmetric Encryption
Building on Finite Non-Abelian Groups**

Rainer Steinwandt
Florida Atlantic University

(Based on joint work with María Isabel González Vasco,
Consuelo Martínez, Jorge L. Villar)

Public Key Encryption

A triple of polynomial time algorithms:

Key generation: probabilistic; given a "key length", outputs secret & public key (pk, sk)

Encryption: probabilistic; given pk and message m , outputs an encryption of m

Decryption: deterministic; given sk and a ciphertext, outputs decryption or an error

Secrecy Requirement

Ciphertext should leak length information only—if a computational assumption holds:

Example: ElGamal in prime order group $\langle g \rangle$

Secret: random $a \in \{1, \dots, \text{ord}(g)\}$


Public: g^a

Encrypting $m \in \langle g \rangle$: $(g^k, g^{ak \cdot m})$ w/ random k .

“If $(g^a, g^k, g^{ak}) \approx (g^a, g^k, g^{\text{rand.}})$, ciphertext tells nothing about plaintext” (DDH)

Malleability

Hiding the plaintext may not be enough:


$$(g^k, g^{ak \cdot m}) \longrightarrow (g^k, g^{ak \cdot m \cdot m'})$$

Adversary can modify message to obtain a “meaningfully related plaintext” (\rightarrow auction)

Theory on provable security:

If adversary can access a decryption oracle,
non-malleability \Leftrightarrow indistinguishable encrypt.

Chosen Ciphertext Attacks

Indistinguishable encryptions under adaptive chosen ciphertext attacks (IND-CCA):

1. attacker gets public key & access to decryption oracle
2. ... fixes equal-length messages m_0, m_1
3. ... gets an encryption of one m_i (random)
4. ... and tries to recover m_i

Goal: public key encryption scheme s.t. under a plausible assumption no ppt algorithm wins this game w/ non-negligible prob.

The Cramer & Shoup Construction

Fact:

A construction of Cramer & Shoup achieves this goal (efficiently) under assumptions building on finite abelian groups.

Hope:

Adapting/generalizing this construction enables use of new hardness assumptions building on finite non-abelian groups.



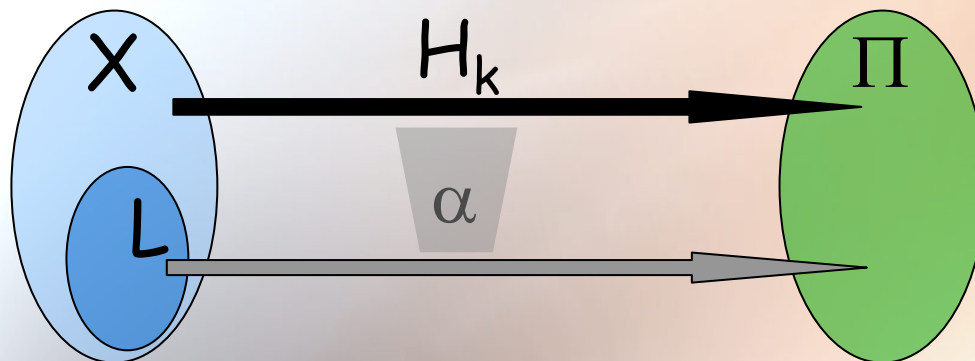
Projective Hash Families

X, Π, S, K : finite non-empty sets

$\alpha: K \rightarrow S$ ("projection of keys")

H : K -indexed family of maps $H_k: X \rightarrow \Pi$

For $L \subseteq X$ we call $(H, K, X, L, \Pi, S, \alpha)$ a **projective hash family (PHF)** for (X, L) iff for all $k \in K$ the restriction $H|_L$ is uniquely determined by $\alpha(k)$.



Smooth & Universal PHFs

A projective hash family is ...

- ◆ **ϵ -universal**: for all $x \in X-L$ and uniformly at random chosen $k \in K$, the probability of guessing $H_k(x)$ from x and $\alpha(k)$ is $\leq \epsilon$

“Outside L , $\alpha(k)$ helps us almost nothing.”

- ◆ **ϵ -universal₂**: ... even if we know some $H_k(x_0)$ value with $x_0 \in X-L$

- ◆ **ϵ -smooth**: ... the prob. distrib. $(x, \alpha(k), \pi)$ and $(x, \alpha(k), H_k(x))$ are ϵ -close (uniformly at random chosen $x \in X-L$, $k \in K$, $\pi \in \Pi$, resp.)
- “ H_k looks on $X-L$ like on the whole of X ”

Subset Membership Problems (I)

Security proofs often use decision problems parameterized with a security parameter l .

Cramer/Shoup framework tries to capture these in a **subset membership problem** specifying for each l an instance distribution.

(... + "some algorithms to get it effective")

Subset Membership Problems (II)

Next to sets $L \subseteq X$, an instance specifies a relation on $L \times W$ —for each $x \in L$ we have a **witness** $w \in W$ proving $x \in L$.

In a **hard membership problem**, we have
(instance descr., x) \approx (instance descr., x')
for $x \in L$ and $x' \in X-L$ uniformly at random.

Associate to each instance of a membership problem a PHF \rightarrow a **hash proof system (HPS)**.

Hash Proof Systems

... also provide “a couple of algorithms”, like

- choosing keys $k \in K$ uniformly at random
- a **private evaluation algorithm** enabling for given $k, x \in X$ the computation of $H_k(x)$
- a **public evaluation algorithm** enabling for given $\alpha(k), x \in L$ and a witness w for x the computation of $H_k(x)$

 **Cramer-Shoup uses strongly smooth HPS**
witness vital for public $H_k(x)$ computation

Cramer/Shoup Public Key Encrypt.

... uses hard subset membership problem M
w/ 2 hash proof systems (strongly smooth/
strongly universal₂ ext.)

Basic construction (w/ Π a group):

Secret: $k \in K$

Public: $\alpha(k) + \text{instance descript.}$

Encrypt $m \in \Pi$:

1. sample random $x \in L$ + witness for x
2. compute $H_k(x)$ w/ public evaluation alg.
3. send $(x, m \cdot H_k(x)) + \text{"proof of integrity"}$

Decrypt: check integrity & recover m

Group Structure Helps

-generic constructions known, e.g., to upgrade a universal HPS into a universal₂ or strongly smooth one.

-Cramer/Shoup: $L \leq X$, Π finite abelian groups, $H \leq \text{Hom}(X, \Pi) \longrightarrow$ such group systems enable more efficient universal₂ construction

Task: Build hard subset membership problem & universal HPS on finite groups

Automorphism Group Systems

An automorphism group system (X, H, α, S) is comprised of:

X, S finite (not necessarily abelian) groups,
 $H \leq \text{Aut}(X)$, $\alpha: H \rightarrow S$ a group homomorphism

For $x \in X$ consider its orbit $[x]$ under the action of $\ker \alpha$, and set $L := \{x \in X: [x] = \{x\}\}$

$L \leq X$ and for $\phi \in H$ the value $\alpha(\phi)$ fixes $\phi|_L$.

Autom. Group Proj. Hash Families

... together with a bijection $h: K \rightarrow H$, we get a(n automorphism group) proj. hash family

An automorphism group system is p -diverse, if $|[x]| \geq p$ holds for all $x \in X-L$.

Useful properties:

- Aut. grp. syst. (X, H, α, S) is p -diverse for the smallest prime p dividing $|\ker \alpha|$
- p -diversity of the aut. group system yields $1/p$ -universality of the proj. hash family.

... Collecting Ingredients

- if $X-L$ is a **single orbit** under the action of $\ker \alpha$, we get $|L|/|X|$ -**smoothness**
- **p-diversity yields dedicated construction guaranteeing $1/p$ -universality₂**

... we can get the projective hash families needed in the Cramer-Shoup construction

... together with a hard subset membership problem this would yield IND-CCA



Getting Examples ...

... that yield something of practical value is unfortunately not that trivial

Less restrictive setting is possible:

in a group action system, H is required to (left-)act on a set X (González Vasco/Villar)

... but so far all practically convincing examples are abelian



Thinking Along the Lines of MST_1

- $[A_1, \dots, A_s]$ a logarithmic signature for $L \leq X$
- $H \leq \text{Aut}(X)$ s.t. L is fixed by each $\phi \in H$
- $\alpha: \phi \rightarrow \phi|_L$ (publish image on log. sig.)
- witness set $W := \{0 \dots |A_1| - 1\} \times \dots \times \{0 \dots |A_s| - 1\}$
- sampling $(x, w) \in L \times W$: "choose random w & take it for pointer into the log. sig."

...in this way we can find aut. group system

... but getting the "complete thing", incl. hard subset membership problem, not obvious

Concluding Remarks

- relevant parts of the Cramer/Shoup framework can be made "non-abelian"
- framework yields no practical example for a non-abelian encryption scheme so far
- w/o random oracle, Cramer/Shoup seems a natural tool for "non-abelian + IND-CCA"

... more insight needed, more work to be done