A new Cramer-Shoup like methodology for group based provably secure encryption schemes

María Isabel González Vasco[1], Consuelo Martínez[2], Rainer Steinwandt[3] and Jorge L. Villar[4]

[1] Área de Matemática Aplicada, Universidad Rey Juan Carlos, c/ Tulipán, s/n, 28933 Madrid, Spain; migonzalez@escet.urjc.es
[2] Departamento de Matemáticas, Universidad de Oviedo, c/Calvo Sotelo, s/n, 33007 Oviedo, Spain; chelo@pinon.ccu.uninovi.es
[3] IAKS, Arbeitsgruppe Systemsicherheit Prof. Beth, Fakultät für Informatik, Universität Karlsruhe, 76128 Karlsruhe, Germany; steinwan@ira.uka.de
[4] Departamento de Matemática Aplicada IV, Universitat Politécnica de Catalunya, Campus Nord, c/Jordi Girona, 1–3, 08034 Barcelona, Spain; jvillar@mat.upc.es

Abstract. A theoretical framework for the design of—in the sense of IND-CCA—provably secure public key cryptosystems taking non-abelian groups as a base is given. Our construction is inspired by Cramer and Shoup's general framework for developing secure encryption schemes from certain language membership problems; thus all our proofs are in the standard model, without any idealization assumptions. The skeleton we present is conceived as a guiding tool towards the construction of secure concrete schemes from finite non-abelian groups (although it is possible to use it also in conjunction with finite abelian groups).

1 Introduction

In the last few years, the outrageous development of cryptanalytic techniques has encouraged the search for theoretical models allowing for mathematical proofs of security. Ideally, a security model should take into account all possible attacks, including those performed on the physical device where the scheme is implemented (such as timing attacks, differential power analysis or attacks relying on the induction of faults) or those that could be carried out with non-standard computing resources like a quantum computer.

One step behind such an ideal model, the nowadays standard notion of security for public key encryption schemes (IND-CCA) abstracts the implementation-dependent characteristics and models the attacker in terms of probabilistic polynomial-time (ppt) algorithms. Building on ideas of Naor and Yung [19], IND-CCA security was introduced by Rackoff and Simon [20], who also presented a scheme secure in this sense. A scheme with similar properties was afterwards designed by Dolev, Dwork, and Naor [9]. Note that, equivalently, instead of IND-CCA sometimes the term IND-CCA2 or the notion of *semantic security against adaptive chosen ciphertext attacks* is used. As a standard reference for further details on formal security notions like IND-CCA1, NM-CPA, etc. we mention the paper of Bellare et al. [3].

Unfortunately, developing practical cryptosystems which can be proven to be IND-CCA secure is a highly non-trivial task, and therefore, idealized models of computation have been introduced in order to obtain simpler proofs yet reasonable security guarantees [10, 4]. The first 'realistic' (that is, practical) proposal without idealization hypothesis was that of Cramer and Shoup [7, 8], which uses the Decision Diffie-Hellman assumption as a base. The same authors gave later a very general construction which in particular led to the design of IND-CCA group theoretic schemes constructed from certain group based primitives called *group systems*. Essentially, such primitives are derived from hard subgroup membership problems of suitable abelian groups.

On the other hand, group theory has lately attracted a lot of attention as a potential source of cryptographic primitives. Having in mind the existing quantum algorithms for factoring integers and computing discrete logarithms, it is indeed worthwhile to explore different areas of mathematics in search of hard problems. Several proposals to use hard problems in non-abelian groups for public key encryption have been made, some based on word or factorization problems [22, 11, 18] and others on variants of the conjugacy problem in braid groups [2, 1, 15, 16]. Unfortunately, almost all of these have been proven insecure in some sense [13, 5, 14, 6]. In [12] common properties of some of these schemes have been exploited to identify a security flaw according to one of the standard security notions (malleability). A sound design framework could be very helpful to prevent this kind of flaws when developing new schemes based on non-abelian groups.

With this purpose in mind, below a theoretical framework for constructing IND-CCA secure public key schemes using finite not necessarily abelian groups is described. Our design is inspired by that of Cramer and Shoup [8, 7], but it is not a generalization of it. It is our aim to provide precise guidelines for developing group-based schemes with a sound theoretical basis, and we hope that the design presented here leads to practical and secure constructions as soon as reasonable hardness assumptions for certain group-based problems are identified.

2 Main tools of Cramer and Shoup's construction

The main building blocks of the public key cryptosystem introduced by Cramer and Shoup are so-called *projective hash families, subset membership problems* and *universal hash proof systems*. We include an informal summary of these notions and refer to [7, 8] for the corresponding definitions.

2.1 Projective hash families

Let X, Π be finite non-empty sets, and K some finite index set. Consider a family $H = \{H_k : X \longrightarrow \Pi\}_{k\in K}$ of mappings from X into Π, and let $\alpha : K \longrightarrow S$ be a map from K into some finite non-empty set S.

With this notation, for a given subset $L \subset X$, we refer to the tuple $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$, as *projective hash family* (PHF) for (X, L) if for all $k \in K$ the restriction of H_k to L is determined by $\alpha(k)$, i.e., for all $x \in L$ and $k_1, k_2 \in K$ the equality $\alpha(k_1) = \alpha(k_2)$ implies $H_{k_1}(x) = H_{k_2}(x)$.

Next, we consider three concepts to limit the amount of information about the behavior of a map H_k on $X \setminus L$, given by $\alpha(k)$:

- We say that $\mathbf{H}$ is ε*-universal* if for any $x \in X \setminus L$ and for a uniformly at random chosen $k \in K$, the probability of correctly guessing $H_k(x)$ from x and $\alpha(k)$ is at most ε. In other words, $\alpha(k)$ determines $H_k\,|_L$ completely, but gives (almost) no information about $H_k\,|_{X\setminus L}$.
- We say $\mathbf{H}$ is ε-universal$_2$ if even knowing (besides $H_k\,|_L$) the value of H_k in some $x^* \in X \setminus L$, for any $x \in X \setminus (L \cup \{x^*\})$ the value of $H_k(x)$ can be guessed correctly with probability at most ε.
- Finally, we say that $\mathbf{H}$ is ε*-smooth* if the probability distributions of $(x, s, \quad H_k(x))$ and (x, s, π), where k, x and π are chosen uniformly at random in K, $X \setminus L$ and Π, respectively, and $s = \alpha(k)$, are ε-close.

2.2 Subset membership problems

Many cryptosystems base their semantic security on a decisional assumption such as the Decision Diffie-Hellman (DDH) assumption or the Quadratic Residuosity (QR) assumption. Most of these assumptions can be formulated in terms of indistinguishability of two probability distributions. Namely, the uniform distribution on a set X and the uniform distribution on a subset $L \subset X$. For instance, if G is a cyclic group of prime order p and g_1 and g_2 are two randomly selected generators of

G, the DDH assumption on G is formalized by setting $X = G \times G$ and $L = \langle (g_1, g_2) \rangle$.

Since computational assumptions are in nature complexity theoretical statements, a complexity parameter $l \in \mathbb{N}_0$, (as the binary length of p in DDH) must be taken into account. Also, for each value of l, there are some possible instances of the same problem. The (random) choice of a particular instance for complexity parameter l is modelled by a samplable probability distribution I_l on the set of instance descriptions. In addition to a set X along with a subset $L \subset X$, an instance description Λ specifies a binary relation $\mathcal{R} \subseteq L \times W$, where W is a so-called *witness test* whose elements provide 'proofs of belonging' to the elements in L, that is, given $x \in L$, there is always a $w \in W$ that can be used to prove that x belongs to L.

Now, a *subset membership problem* $\mathcal{M}$ specifies a collection of distributions $(I_l)_{l \in \mathbb{N}_0}$ on the set of instance descriptions along with several sampling and verifying algorithms:

- a ppt algorithm called the *instance generator* that on input 1^l, outputs a description $\Lambda = \Lambda[X, L, W, \mathcal{R}]$ as just described;
- a ppt algorithm which, upon input of 1^l and a certain instance $\Lambda = \Lambda[X, L, W, \mathcal{R}]$, outputs a random $x \in L$ and a witness $w \in W$ for x (*subset sampling algorithm*);
- a deterministic polynomial time algorithm that takes as input 1^l, an instance $\Lambda = \Lambda[X, L, W, \mathcal{R}]$ and a binary string ζ, and checks whether ζ is a valid encoding of an element $x \in X$.

Moreover, $\mathcal{M}$ is *hard* if the probability distributions (Λ, x) and (Λ, x'), where $\Lambda = \Lambda[X, L, W, \mathcal{R}]$ is the output of the instance generator and x, x' are uniformly distributed on L and $X \setminus L$ respectively, are polynomially indistinguishable.

2.3 Universal hash proof systems

A *hash proof system* (HPS) $\mathcal{P}$ is a rule which for a subset membership problem $\mathcal{M}$ associates to each instance $\Lambda = \Lambda[X, L, W, \mathcal{R}]$ of $\mathcal{M}$ a projective hash family $(H, K, X, L, \Pi, S, \alpha)$ for (X, L). In addition, $\mathcal{P}$ provides the following sampling and verifying algorithms which are polynomial in the complexity parameter l:

- a probabilistic algorithm that on input 1^l and Λ (with non-zero probability according to the corresponding distribution I_l) outputs $k \in K$ chosen uniformly at random;

– a deterministic algorithm that on input 1^l, Λ and k as above, outputs $\alpha(k) \in S$;
– a deterministic *private evaluation algorithm* that on input l, Λ, k as above, and $x \in X$ outputs $H_k(x) \in \Pi$;
– a deterministic *public evaluation algorithm* that on input 1^l, Λ as above, $s \in \alpha(K)$ and $x \in L$ together with a witness $w \in W$ for x, outputs $H_k(x) \in \Pi$ (where $\alpha(k) = s$);
– a deterministic algorithm that on input 1^l, Λ as above and a bitstring ζ determines if ζ is a valid encoding of an element of Π.

A hash proof system $\mathcal{P}$ is referred to as *ε-universal*, if the PHFs it associates to the instances of a subset membership problem $\mathcal{M}$ are 'almost' *ε-universal.* Namely, consider $\varepsilon : \mathbb{N}_0 \longrightarrow \mathbb{R}_{>0}$, a function of the complexity parameter l. Then we call $\mathcal{P}$ *ε-universal* (resp. *universal$_2$*, *smooth*) if there exists a negligible function $\delta(l)$ such that for all $l \in \mathbb{N}_0$ and all instances Λ of $\mathcal{M}$, the PHF $\mathbf{H}$ associated to Λ by $\mathcal{P}$ is $\delta(l)$-close to an $\varepsilon(l)$-universal (resp. universal$_2$, smooth) PHF. Moreover, if this is the case, and $\varepsilon(l)$ is a negligible function, then we say that $\mathcal{P}$ is *strongly* universal (resp. universal$_2$, smooth). Finally, it is convenient to provide an extended notion of hash proof systems obtained by simply replacing the sets X and L by $X \times E$ and $L \times E$ for a a suitable finite set E. Also, in these *extended hash proof systems* a value $e \in E$ is passed as an additional input to both the private and the public evaluation algorithm.

It is worth noticing that if a HPS is strongly universal and the underlying subset membership problem is hard, then the problem of evaluating $H_k(x)$ for random $k \in K$ and arbitrary $x \in X$ given only x and $\alpha(k)$ is also hard. Thus, the role of the witness in the public evaluation algorithm becomes clear: without w there is no way to efficiently compute $H_k(x)$.

2.4 Cramer and Shoup's IND-CCA secure public key encryption scheme

Roughly speaking, in the scheme proposed by Cramer and Shoup [7, 8] a message $m \in \Pi$ is encrypted by using $H_k(x)$ as a one time pad; while the value of k is kept secret, x and $\alpha(k)$ are made public. More precisely, given a strongly smooth HPS for a hard subset membership problem, the secret key of the encryption scheme is $k \in K$, and the public key consists of $s = \alpha(k)$ along with the instance description. The message space is Π. To encrypt a message $m \in \Pi$, first a random pair $(x, w) \in L \times W$ is generated, so that w is a witness for x. Next, by means of the public evaluation algorithm, the value $H_k(x)$ is computed; the ciphertext is the pair $(x, m \cdot H_k(x))$, where $\cdot$ is a suitable group operation. Implicitly, it is assumed that Π is a group where elements can be efficiently inverted and multiplied.

Clearly, the holder of k can retrieve $H_k(x)$ by using the private evaluation algorithm, and therewith the message. On the other hand, since the subset membership problem is hard, there is no way for a polynomially bounded adversary to distinguish between a well-formed ciphertext and a fake ciphertext obtained by choosing $x \in X \setminus L$ instead of $x \in L$. However, due to the smoothness of the HPS, since k is unknown, $H_k(x)$ is close to be uniformly distributed on Π, so the message is nearly perfectly hidden. Therefore, no information about the plaintext can be obtained in polynomial time by a passive adversary.

IND-CCA security is achieved by appending to the ciphertext a 'proof of integrity' obtained from a strong universal$_2$ extended HPS. The set E in the definition of this extended HPS is just the message space Π. More formally:
Let $\mathcal{M}$ be a hard subset membership problem and $\mathcal{P}, \hat{\mathcal{P}}$ be two HPSs for $\mathcal{M}$, strongly smooth and strongly universal$_2$ extended respectively. An instance of these objects is described by an instance $\Lambda[X, L, W, \mathcal{R}]$ of $\mathcal{M}$ and two instances $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$ and $\hat{\mathbf{H}} = (\hat{H}, \hat{K}, X \times \Pi, L \times \Pi, \hat{\Pi}, \hat{S}, \hat{\alpha})$ of $\mathcal{P}$ and $\hat{\mathcal{P}}$, respectively. Note that the instances of $\mathcal{P}$ and $\hat{\mathcal{P}}$ must share the sets X, L and W and the sampling algorithm. Once the above parameters are fixed, the algorithms of the encryption scheme can be described as follows:

Key generation Choose $k \in K$ and $\hat{k} \in \hat{K}$ uniformly at random, compute $s = \alpha(k) \in S$, $\hat{s} = \hat{\alpha}(\hat{k}) \in \hat{S}$ and output two pairs $(s, \hat{s})$—the public key—and $(k, \hat{k})$—the private key.

Encryption To encrypt a plaintext $m \in \Pi$, first generate $x \in L$ and a corresponding witness $w \in W$ by means of the subset sampling algorithm provided by $\mathcal{M}$. Then compute

- $\pi = H_k(x)$ (from x, s and w, by using the public evaluation algorithm provided by $\mathcal{P}$)
- $e = m \cdot \pi \in \Pi$ and $\hat{\pi} = \hat{H}_{\hat{k}}(x, e)$ (from $\hat{s}, x, e$ and w, by using the public evaluation algorithm provided by $\hat{\mathcal{P}}$).

The output ciphertext is the tuple $(x, e, \hat{\pi})$.

Decryption algorithm To decrypt the received ciphertext $(x, e, \hat{\pi})$,

- compute $\hat{\pi}' = \hat{H}_{\hat{k}}(x, e) \in \hat{\Pi}$ (by means of the private evaluation algorithm of $\hat{\mathcal{P}}$),

– check whether $\hat{\pi} = \hat{\pi}'$ and, if not, output *reject* and halt. Otherwise, compute $\pi = H_k(x) \in \Pi$ (by means of the private evaluation algorithm of $\mathcal{P}$) as well as the plaintext $m = e \cdot \pi^{-1} \in \Pi$.

This algorithm is also supposed to recognize and reject bitstrings that do not correspond to properly formed ciphertexts, i. e., bitstrings that do not encode an element of $X \times \Pi \times \hat{\Pi}$.

3 Main tools of a non-abelian construction based on group automorphisms

In [8], Cramer and Shoup give a group-theoretic construction for deriving universal projective hash families from so-called *group systems*. Their construction is based on the use of finite abelian groups, and they prove that, if the group system has certain properties, then the corresponding PHF is ε-universal$_2$. We establish the same result for a different group-based primitive, which we call *automorphism group system*.

3.1 Automorphism group systems

Let X be a (not necessarily abelian) group. Multiplicative notation will be used for all groups, thus the unit element will be denoted by 1. Let H be a finite subgroup of $\mathrm{Aut}(X)$, S some finite group and $\chi : H \longrightarrow S$ a group homomorphism. Note that for any $\phi \in H$, $\chi(\phi)$ gives some (limited) information about ϕ.

Definition 1. *Let X, H, S and χ be defined as above. Then the tuple (X, H, χ, S) is called an* automorphism group system*.*

For any $\phi \in H$, let $[\phi] = \chi^{-1}(\chi(\phi))$ denote the class of ϕ in $H/\ker\chi$. Obviously, $|[\phi]| = |\ker\chi|$, and for any $x \in X$ and $\phi \in H$ we have

$$[\phi](x) = \{\psi(x) \mid \psi \in [\phi]\} = \phi((\ker\chi)(x)).$$

Denoting the orbit of x under the action of $\ker\chi$ by $[x]$, we have $|[\phi](x)| = |\phi([x])| = |[x]|$, as ϕ is a bijection. Clearly, $x \in [x]$ and hence $|[x]| \geq 1$; denote by L the set $\{x \in X \mid |[x]| = 1\}$, that is $\{x \in X \mid [x] = \{x\}\}$. Then it is trivial to check that L is a subgroup of X. Note also that, if $x, y \in X$ are in the same class modulo L, i.e., if $xL = yL$, then $|[x]| = |[y]|$.

Observe that the restriction of ϕ to L only depends on $\chi(\phi)$ and that $\ker\chi \subseteq \mathrm{Stab}(L)$ although they are not necessarily equal.

As the systems above will be useful for us if χ gives little information about the action of H on $X \setminus L$, we will be particularly interested in those systems for which the $(\ker\chi)$-orbits of elements in $X \setminus L$ are large.

Definition 2. *Let $p > 1$ be a positive integer. The automorphism group system (X, H, χ, S) is p-*diverse *if $|[x]| \geq p$ for all $x \in X \setminus L$.*

Lemma 1. *Let (X, H, χ, S) be an automorphism group system, and let p be the smallest prime dividing $|\ker \chi|$. Then (X, H, χ, S) is p-diverse.*

Proof. Note that $\ker \chi$ acts on X, and thus $|[x]|$ divides $|\ker \chi|$, so if $x \in X \setminus L$ (i.e., if $|[x]| \neq 1$) then $|[x]|$ is at least p. □

To get a better intuition of the notion of automorphism group system, we conclude this section with a simple (abelian) example in a setting analogue to [7, Section 7.4.2 Example 2]:

Example 1. Denote by X some cyclic group of composite order $a = b \cdot b'$ with $b < b'$ being different prime numbers, and let L be the (unique) subgroup of X of order b. Then X is isomorphic to $\mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/b'\mathbb{Z}$, and the automorphism group $H := \mathrm{Aut}(X)$ can be identified with $\mathbb{Z}/(b-1)\mathbb{Z} \times \mathbb{Z}/(b'-1)\mathbb{Z}$.

Thus, using this identification, define χ as the corresponding natural projection

$$\begin{array}{rcl} \chi : \quad H & \longrightarrow & S := \mathbb{Z}/(b-1)\mathbb{Z} \\ (h_1, h_2) & \longmapsto & h_1 \end{array} .$$

Thus, the kernel of χ is isomorphic to $\mathbb{Z}/(b'-1)\mathbb{Z}$, and obviously each element of L is stabilized by $\ker \chi$. Moreover, one easily checks that any element having only a single image under $\ker \chi$ is already contained in L. In other words (X, H, χ, S) is an automorphism group system in the sense of Definition 2, and $L = \{x \in X \mid |[x]| = 1\}$. It is also easy to check that this automorphism group system is $(b'-1)$-diverse.

Remark 1. Note that Example 1 can easily be generalized to the case $X = A \times B$ for some not necessarily abelian finite groups A and B, $H = \mathrm{Aut}(A) \times \mathrm{Aut}(B)$, $S = \mathrm{Aut}(A)$ and χ the corresponding projection. Actually, in Example 1 we have $\gcd(|A|, |B|) = 1$, and therefore $H = \mathrm{Aut}(A) \times \mathrm{Aut}(B) = \mathrm{Aut}(X)$.

3.2 Automorphism group projective hash families

As it was the case for abelian group systems [7, 8], a projective hash family can be built from an automorphism group system by providing some additional elements:

Let us consider an automorphism group system (X, H, χ, S), and denote by $\hbar : K \to H$ a bijection from a suitable index set K (which will later serve as the private key space). Noting that $\chi(\hbar(k))$ determines the action of $\hbar(k)$ on L completely, it is easy to see that the tuple $(H, K, X, L, X, S, \chi \circ \hbar)$ is a projective hash family.

Definition 3. *Any PHF constructed from an automorphism group system as described above is called* automorphism group projective hash family *(APHF).*

An automorphism group projective hash family is made explicit by the tuple $(X, H, K, S, \chi, \hbar)$.

It is our aim to prove that, if the automorphism group projective hash family has certain nice properties, the resulting APHF will be ε-universal for some $\varepsilon > 0$. We start by demonstrating that for any $x \in X$, choosing $k \in K$ uniformly at random (that is, choosing uniformly at random a homomorphism in H), given $\chi(\hbar(k))$, there are exactly $|[x]|$ equally probable candidates for $(\hbar(k))(x)$.

Lemma 2. *Let* (X, H, χ, S) *be an automorphism group system and let* $x \in X$*. If* $\phi \in H$ *is chosen uniformly at random, once* $s = \chi(\phi)$ *is given then* ϕ *is uniformly distributed on the coset* $\chi^{-1}(s)$ *and* $\phi(x)$ *is uniformly distributed on the set* $\{\psi(x) \mid \psi \in \chi^{-1}(s)\}$*, that is, on a set of cardinality equal to* $|[x]|$.

Proof. Clearly, as ϕ is chosen uniformly at random, once we fix $s = \chi(\phi)$, the resulting distribution is uniform on $\chi^{-1}(s)$. Moreover, for any $x \in X$, $\phi(x)$ is uniformly distributed on

$$\{\psi(x) \mid \psi \in \chi^{-1}(s)\}$$

provided that the sets

$$S_y = \{\psi \in \chi^{-1}(s) \mid \psi(x) = y\}$$

for all $y \in \{\psi(x), \psi \in \chi^{-1}(s)\}$ are of the same size. But this is straightforward to see, as all S_y are left cosets modulo $\ker \chi \cap \mathrm{Stab}(\{x\})$. □

Proposition 1. *Let* $\mathbf{H} = (X, H, K, S, \chi, \hbar)$ *be an automorphism group projective hash family.*

If the underlying automorphism group system (X, H, χ, S) *is* p*-diverse then* $\mathbf{H}$ *is* $1/p$*-universal.*

Proof. From Lemma 2, for any $x \in X \setminus L$, the probability of guessing the right value of $(\hbar(k))(x)$ for a random choice of $k \in K$ given $\chi(\hbar(k))$ is $1/|[x]|$, that is at most $1/p$. □

In [8] a generic method to obtain a smooth projective hash family from any universal projective hash family, taking advantage of the Left-over Hash Lemma, is described. Nevertheless, in some special cases, the smoothness can be guaranteed directly.

Proposition 2. *Let* $\mathbf{H} = (X, H, K, S, \chi, \hbar)$ *be an automorphism group projective hash family. If the whole set* $X \setminus L$ *is a single orbit under the action of* $\ker \chi$ *then* $\mathbf{H}$ *is* $|L|/|X|$*-smooth.*

Proof. Let $x \in X \setminus L$. From Lemma 2, $(\hbar(k))(x)$ is uniformly distributed on a set of size $|[x]| = |X \setminus L|$. Then, the statistical distance between $(\hbar(k))(x)$ and the uniform distribution on X is

$$\frac{1}{2} \sum_{x \in X \setminus L} \left| \frac{1}{|X| - |L|} - \frac{1}{|X|} \right| + \frac{1}{2} \sum_{x \in L} \frac{1}{|X|} = \frac{|L|}{|X|},$$

thus the probability distribution of $(\hbar(k))(x)$ is $|L|/|X|$-close to the uniform distribution on X □

3.3 Universal$_2$ extended projective hash families

In [8], the authors outline a generic transformation from any ε-universal projective hash family to an ε-universal$_2$ extended projective hash family. But in the case of automorphism group projective hash families there is a more efficient way to achieve this goal.

Let $\mathbf{H} = (X, H, K, S, \chi, \hbar)$ be an automorphism group projective hash family such that the underlying automorphism group system (X, H, χ, S) is p-diverse. Let q be the smallest prime factor of $|H|$. Further on, denote by n a positive integer and by E a finite set. Let us define a new extended projective hash family $\hat{\mathbf{H}}$ by means of $n+1$ independent copies of $\mathbf{H}$ and a "gluing" function $g_\gamma^H : H^{n+1} \to H$ defined by:

$$g_\gamma^H(\phi_0, \ldots, \phi_n) := \phi_0 \circ \phi_1^{\gamma_1} \circ \cdots \circ \phi_n^{\gamma_n}$$

where $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^n$ and $\phi_i^{\gamma_i}(x) := \underbrace{\phi_i \circ \cdots \circ \phi_i}_{\gamma_i}(x)$.

Similarly, we define $g_\gamma^S : S^{n+1} \to S$ by

$$g_\gamma^S(s_0, \ldots, s_n) := \chi(g_\gamma^H(\phi_0, \ldots, \phi_n)) = s_0 s_1^{\gamma_1} \cdots s_n^{\gamma_n},$$

where $\phi_j \in \chi^{-1}(s_j)$ for all $j = 0, \ldots, n$.

Now, $\hat{K} = K^{n+1}$, $\hat{S} = S^{n+1}$ and the natural extensions $\hat{\chi}$ of χ and $\hat{\hbar}$ of $\hbar$ are used. The set X is extended to $\hat{X} = X \times E$. Further on, given $\hat{k}$, we define $\Phi_{\hat{k}} : X \times E \longrightarrow X$ by

$$\Phi_{\hat{k}}(x, e) := g^H_{\Gamma(x,e)}(\hat{\hbar}(\hat{k}))(x),$$

where $\Gamma : (x, e) \mapsto (\Gamma_1(x, e), \dots, \Gamma_n(x, e))$ is an injective map from $X \times E$ into $\{0, \dots, q-1\}^n$. Let us denote by $\hat{H}$ the set $\{\Phi_{\hat{k}} \mid \hat{k} \in \hat{K}\}$.

The soundness of our construction will rely on the commutativity of the following diagram:

$$\begin{tikzcd} H^{n+1} \arrow[r, "g^H_\gamma"] \arrow[d, "\hat{\chi}"'] & H \arrow[d, "\chi"] \\ \hat{S} \arrow[r, "g^S_\gamma"'] & S \end{tikzcd}$$

It can be shown that

$$\hat{\mathbf{H}} = (\hat{H}, \hat{K}, X \times E, L \times E, X, \hat{S}, \hat{\chi} \circ \hat{\hbar})$$

is a $1/p$-universal$_2$ projective hash family. Recall that this actually means that for any $x \in X \setminus L$ and $e \in E$ if $\hat{k} \in \hat{K}$ is chosen uniformly at random and $\hat{\chi}(\hat{\hbar}(\hat{k}))$, $\Phi_{\hat{k}}(x^*, e^*)$ are known (for some $x^* \in X \setminus (L \cup \{x\})$ and $e^* \in E$), the probability of guessing $\Phi_{\hat{k}}(x, e)$ correctly is smaller than $1/p$.

We start by obtaining an analogue of Lemma 2.

Lemma 3. *Let $\hat{\mathbf{H}}$ be as above, $x \in X$ and $e \in E$. Then, if $\hat{\phi} \in H^{n+1}$ is chosen uniformly at random, once $\hat{s} = \hat{\chi}(\hat{\phi})$ is fixed, then $\phi = g^H_{\Gamma(x,e)}(\hat{\phi})$ is uniformly distributed on the coset $\chi^{-1}(s)$, where $s = g^S_{\Gamma(x,e)}(\hat{s})$. Moreover, $\phi(x)$ is uniformly distributed on the set $\{\psi(x) \mid \psi \in \chi^{-1}(s)\}$, that is, on a set of cardinality equal to $|[x]|$.*

Proof. It is clear that in the conditional probability space, ϕ is uniformly distributed on the set $g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s}))$. Let us show that this set is just the coset $\chi^{-1}(s)$. It is clear that $g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s})) \subseteq \chi^{-1}(s)$ since $\chi(g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s}))) = g^S_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{\chi}(\hat{s}))) = s$. Conversely, $g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s}))$ contains a whole coset modulo $\ker \chi$. To see this, pick an element $\psi \in g^H_{\Gamma(x,e)}(\hat{\chi}^{-1}(\hat{s}))$. Then, there exists $\hat{\psi} = (\psi_0, \psi_1, \dots, \psi_n) \in \hat{\chi}^{-1}(\hat{s})$ such that $\psi = g^H_{\Gamma(x,e)}(\hat{\psi})$. For each $\eta \in \ker \chi$, $\eta \circ \psi = g^H_{\Gamma(x,e)}(\eta \circ \psi_0, \psi_1, \dots, \psi_n)$ that is also in $\hat{\chi}^{-1}(\hat{s})$. From this point, the proof proceeds exactly as in Lemma 2. $\square$

Proposition 3. *If* (X, H, χ, S) *is* p*-diverse then* $\hat{\mathbf{H}}$ *is a* $1/p$*-universal projective hash family.*

Proof. From Lemma 3, for any $x \in X \setminus L$ and $e \in E$, the probability of guessing the right value of $\Phi_{\hat{k}}(x, e) = g^H_{\Gamma(x,e)}(\hat{\hbar}(\hat{k}))(x)$ for a random choice of $\hat{k} \in \hat{K}$ given $\hat{\chi}(\hat{\hbar}(\hat{k}))$ is $1/|[x]|$, that is at most $1/p$. □

The next proposition shows that $\hat{\mathbf{H}}$ is also universal$_2$ (see Appendix A for a proof):

Proposition 4. *If* (X, H, χ, S) *is* p*-diverse then* $\hat{\mathbf{H}}$ *is a* $1/p$*-universal*$_2$ *projective hash family.*

Equipped with these results, we can now mimic Cramer and Shoup's (abelian) construction. Given a hard subset membership problem $\mathcal{M}$ and suitable automorphism group systems, we can construct, analogously as it is done in [7, 8], two HPSs for $\mathcal{M}$, $\mathcal{P}$ and $\hat{\mathcal{P}}$, strongly smooth and strongly universal$_2$ extended respectively. Then, with the same arguments as in the security proof of the general Cramer and Shoup construction, we obtain:

Proposition 5. *Let* $\mathcal{M}$ *be a hard subset membership problem,* $\mathcal{P}$ *and* $\hat{\mathcal{P}}$ *strongly smooth resp. strongly universal*$_2$ *extended HPSs for* $\mathcal{M}$ *constructed from automorphism group systems.*

Then the public key encryption scheme described in Section 2.4 is secure in the sense of IND-CCA.

4 Deriving examples of provably secure public key encryption schemes

As pointed out, e.g., by Shpilrain in [21], some investigation should still be devoted to the construction of group theoretical schemes with satisfactory security guarantees. At the moment we cannot provide a practical new provably secure public key scheme based on non-abelian groups and the above framework. In the following, we restrict to outlining a possible methodology for designing a cryptosystem fitting our framework. One plausible approach to deriving examples is as follows:

Find a suitable decisional problem. Take, e. g., the decisional Diffie-Hellman problem in a cyclic group $G = \langle g \rangle$ of prime order q.

Represent it as a subset membership problem. For instance: $X = G \times G$ and $L = \langle (g, g^c) \rangle$, for some secret $c \in \{1, \dots, q-1\}$. Thus, L can be seen as a line in $GF(q)^2$ generated by the vector $(1, c)$.

Study a related automorphism group which would fix the subset elements. Take, for the case above, the subgroup of $\mathrm{GL}(2,q)$ that fixes L. That is, the group formed by the matrices that fix the vector $(1,c)$. This will act as the kernel of the homomorphism χ. As this subgroup is not necessarily normal, we take as H its normalizer in $\mathrm{GL}(2,q)$, which has order $q(q-1)^2$.

Construct χ accordingly.

Of course, all these steps have to be done in such a way that the final construction is computationally feasible, so that the required sampling and evaluation algorithms for the encryption scheme can be provided.

The above automorphism group system can be used directly to derive a projective hash family which would however be neither universal nor smooth, but some slight modifications allow to achieve these two properties. Nevertheless, we do not encourage the construction of a hash proof system from it due to the lack of efficiency of some of the required algorithms.

Also, the example above is in some sense 'close' to the abelian case (which, in the end, inspires this construction). However, based on the above methodology one can also think of similar constructions that are genuinely non-abelian. To this aim, we recall the definition of a logarithmic signature, first given by [17]:

Definition 4. *Let L be a finite group. Next, denote by $\xi = [\xi_1, \dots, \xi_s]$ a sequence of length $s \in \mathbb{N}_0$ such that each ξ_i ($1 \leq i \leq s$) is itself a sequence $\xi_i = [\xi_{i0}, \dots, \xi_{ir_i-1}]$ with $\xi_{ij} \in L$ ($0 \leq j < r_i$) and $r_i \in \mathbb{N}_0$.*
Then we call ξ a logarithmic signature *for L if each $g \in L$ is represented uniquely as a product*

$$g = \xi_{1j_1} \cdots \xi_{sj_s} \tag{1}$$

with $\xi_{ij_i} \in \xi_i$ ($1 \leq i \leq s$).

Example 2. Suppose we have at hand a hard subset membership problem $\mathcal{M}$ which for each input $l \in \mathbb{N}_0$ selects an instance constructed as follows: Let X be a non-abelian group, $H \leq \mathrm{Aut}(X)$ and $\xi = [\xi_1, \dots, \xi_s]$ a logarithmic signature for a subgroup L of X, H-invariant (i.e., $\phi(L) = L \; \forall \phi \in H$). Suppose that factoring elements according to ξ is a hard computational problem.

Moreover, let $W := A_{r_1} \times \cdots \times A_{r_s}$ where $|\xi_i| = r_i$ and A_r stands for the set $\{0, \dots, r-1\}$. Define the bijection

$$\begin{array}{rccc} \beta : & W & \longrightarrow & L \\ & (w_1, \dots, w_s) & \longmapsto & \xi_{1w_1} \cdots \xi_{sw_s} \end{array}.$$

The sampling algorithm just chooses a random $w \in W$ and computes $x = \beta(w)$. Now let us describe an automorphism group system for X and L: Assume H is such that that given $\phi \in H$ the images $\phi(\xi_{ij})$, $j = 0, \ldots, r_i - 1$, $i = 1, \ldots, s$ give no information about the action of ϕ on $X \setminus L$. Suppose also that $\phi(\xi)$ induces a polynomial time factorization of $\phi(L)$ for all $\phi \in H$[5]. Let $\hbar$ be an efficiently computable bijection defined between some index set K and H.

Moreover, take $S := H|_L$ and $\chi : H \longrightarrow S$ the natural projection, i.e. $\chi(\phi) := \phi|_L$. Note that the image $\chi(\phi)(x)$ can be efficiently computed for any $x \in L$ given a witness $(w_1, \ldots, w_s)$ for x and the images $\phi(\xi_{iw_i})$ for $i = 1, \ldots, s$. Thus, in practice, $\chi(\phi)$ may be specified by $\phi(\xi)$. Clearly, (X, H, χ, S) is an automorphism group system (see Section 3.1).

Now, from a good enough automorphism group system (i. e., p-diverse for some large prime p), two PHFs, $\mathbf{H}$ and $\hat{\mathbf{H}}$, can be constructed as in Sections 3.2 and 3.3. Then, if there exist efficient algorithms for sampling, public and private evaluation, the resulting encryption scheme will be secure in the sense of IND-CCA.

As a final remark on this example, let us suppose the group H is a subgroup of $\mathrm{Inn}(X)$, that is, for each $\phi \in H$ there exists a certain $a \in X$ so that $\phi(x) = axa^{-1}$. For the scheme to be secure, a special kind of *simultaneous conjugacy problem* must be hard to solve in L. Also, it must be possible to produce *hard* logarithmic signatures of L which could be used as parts of the public keys.

Examples of schemes already proposed relying on similar assumptions are the MST_2 scheme [18] and the key exchange proposed by Anshel et al. in [2]. However, even if the underlying mathematical problems used as a base could be considered hard, such constructions would not be provably secure in the sense of IND-CCA.

5 Conclusions

We have given a theoretical framework which, if sound hardness assumptions are identified, may lead to the construction of IND-CCA public key encryption schemes based on non-abelian groups. The main tool we introduced are *automorphism group systems* for deriving projective hash families from non-abelian groups. The idea used here parallels Cramer and Shoup's abelian construction based on *group systems*. As in their

[5] This last condition could be avoided using the generic transformation from [8].

framework, we give criteria for choosing suitable automorphism group systems in order to obtain useful (i.e. universal) projective hash families. In principle, our model may also help in developing new examples of IND-CCA secure schemes based on abelian groups; it is however especially interesting as a design guide for developing new tools in non-abelian cryptography. Up until now, cryptosystems based on non-abelian groups often turned out to have security flaws which are independent of the soundness of the underlying mathematical assumptions; it is our aim that this design supplies a useful tool to overcome such problems. Unfortunately, so far we cannot offer a practical example of a new public key encryption scheme derived from non-abelian groups in our framework. Having in mind the goal of identifying new mathematical primitives offering provably secure encryption schemes, however, we think it is certainly worthwhile to explore the existence of automorphism group systems and hard subset membership problems based on non-abelian groups fitting our framework.

References

1. I. Anshel, M. Anshel, B. Fisher, and D. Goldfeld. New Key Agreement Protocols in Braid Group Cryptography. In *CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 13–27, Berlin, Heidelberg, 2001. Springer.
2. I. Anshel, M. Anshel, and D. Goldfeld. An algebraic method for public-key cryptography. *Mathematical Research Letters*, 6:1–5, 1999.
3. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. In *Advances in Cryptology, Proceedings of CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 26–45. Springer, 1998.
4. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM Conference on Computer and Communications Security*, pages 62–73, 1993.
5. J.-M. Bohli, M.I. González Vasco, C. Martínez, and R. Steinwandt. Weak Keys in MST_1. *Designs, Codes and Cryptography*, to appear.
6. J.H. Cheon and B. Jun. Diffie-Hellman Conjugacy Problem on Braids. Cryptology ePrint Archive: Report 2003/019, 2003. Electronically available at `http://eprint.iacr.org/2003/019/`.
7. R. Cramer and V. Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. Cryptology ePrint Archive: Report 2001/085, 2001. Electronically available at `http://eprint.iacr.org/2001/085/`.
8. R. Cramer and V. Shoup. Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. In Lars Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64. Springer, 2002.
9. D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. *SIAM Journal on Computing*, 30:391–437, 2000.

10. A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. In *Advances in cryptology—CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1987.
11. M. Garzon and Y. Zalcstein. The Complexity of Grigorchuk groups with application to cryptography. *Theoretical Computer Science*, 88:83–98, 1991.
12. M.I. González Vasco, C. Martínez, and R. Steinwandt. Towards a Uniform Description of Several Group Based Cryptographic Primitives. *Designs, Codes and Cryptography*, 33:215–226, 2004.
13. M.I. González Vasco and R. Steinwandt. Reaction Attacks on Public Key Cryptosystems Based on the Word Problem. *Applicable Algebra in Engineering, Communication and Computing*, 14:335–340, 2004.
14. D. Hofheinz and R. Steinwandt. A Practical Attack on Some Braid Group Based Cryptographic Primitives. In *Public Key Cryptography, 6th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2003 Proceedings*, volume 2567 of *Lecture Notes in Computer Science*, pages 187–198. Springer, 2003.
15. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang, and C. Park. New Public-Key Cryptosystem using Braid Groups. In *Advances in Cryptology. Proceedings of CRYPTO 2000*, volume 576 of *Lecture Notes in Computer Science*, pages 166–183. Springer, 2000.
16. H.K. Lee, H.S. Lee, and Y.R. Lee. An Authenticated Group Key Agreement Protocol on Braid Groups. *Cryptology ePrint Archive: Report 2003/018*, 2003. Electronically available at `http://eprint.iacr.org/2003/018/`.
17. S.S. Magliveras and N.D. Memon. Algebraic properties of cryptosystem PGM. *Journal of Cryptology*, 5:167–183, 1992.
18. S.S. Magliveras, D.R. Stinson, and T. Trung. New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups. *Journal of Cryptology*, 15:285–297, 2002.
19. M. Naor and M. Yung. Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 427–437. ACM Press, 1990.
20. C. Rackoff and D. Simon. Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In *Advances in Cryptology — CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 433–444. Springer, 1992.
21. V. Shpilrain. Assessing security of some group based cryptosystems. Cryptology ePrint Archive: Report 2003/123, 2003. Electronically available at `http://eprint.iacr.org/2003/123/`.
22. N.R. Wagner and M.R. Magyarik. A Public Key Cryptosystem Based on the Word Problem. In *Advances in Cryptology: Proceedings of CRYPTO 84*, volume 196 of *Lecture Notes in Computer Science*, pages 19–36. Springer, 1985.

A Proof of Proposition 4

Proof. Let us suppose as above that $\hat{k} \in \hat{K}$ is selected uniformly at random and $\hat{s} = (s_0, \ldots, s_n) = \hat{\chi}(\hat{\hbar}(\hat{k}))$ is given. Then $\hat{\phi} = \hat{\hbar}(\hat{k}) = (\phi_0, \ldots, \phi_n)$ is also uniformly distributed on $\hat{\chi}^{-1}(\hat{s})$.

In order to guarantee that $\hat{\mathbf{H}}$ is $1/p$-universal$_2$, it suffices to show the independence of the two random variables $\phi = g^H_{\Gamma(x,e)}(\hat{\phi})$ and $\phi^* = g^H_{\Gamma(x^*,e^*)}(\hat{\phi})$, for any $e, e^* \in E$, $x \in X \setminus L$ and $x^* \in X \setminus \{x\}$.

From Lemma 3, ϕ and ϕ^* are uniformly distributed on $\chi^{-1}(s)$ and $\chi^{-1}(s^*)$, respectively, where $s := g^S_{\Gamma(x,e)}(\hat{s})$ and $s^* := g^S_{\Gamma(x^*,e^*)}(\hat{s})$. Now let i be the smallest integer such that $\Gamma_i(x,e) \neq \Gamma_i(x^*,e^*)$, that surely exists since Γ is injective. Now, for any fixed values $\phi_j \in \chi^{-1}(s_j)$ for $j = 1, \dots, i-1, i+1, \dots, n$ let us consider the map

$$\begin{array}{c} \triangle_i : \chi^{-1}(s_0) \times \chi^{-1}(s_i) \longrightarrow \chi^{-1}(s) \times \chi^{-1}(s^*) \\ (\phi_0, \phi_i) \qquad \longrightarrow \qquad (\phi, \phi^*), \end{array}$$

where, as above, $\phi = g^H_{\Gamma(x,e)}(\hat{\phi})$ and $\phi^* = g^H_{\Gamma(x^*,e^*)}(\hat{\phi})$. By defining

$$\begin{aligned} \psi_L &= \phi_1^{\Gamma_1(x,e)} \circ \cdots \circ \phi_{i-1}^{\Gamma_{i-1}(x,e)} = \phi_1^{\Gamma_1(x^*,e^*)} \circ \cdots \circ \phi_{i-1}^{\Gamma_{i-1}(x^*,e^*)}, \\ \psi_R &= \phi_{i+1}^{\Gamma_{i+1}(x,e)} \circ \cdots \circ \phi_n^{\Gamma_n(x,e)} \qquad \text{and} \\ \psi_R^* &= \phi_{i+1}^{\Gamma_{i+1}(x^*,e^*)} \circ \cdots \circ \phi_n^{\Gamma_n(x^*,e^*)} \end{aligned}$$

we can write

$$\triangle_i(\phi_0, \phi_i) = (\phi_0 \circ \psi_L \circ \phi_i^{\Gamma_i(x,e)} \circ \psi_R, \phi_0 \circ \psi_L \circ \phi_i^{\Gamma_i(x^*,e^*)} \circ \psi_R^*).$$

The map $\triangle_i$ is injective. Indeed, consider two pairs (ϕ_0, ϕ_i) and $(\bar{\phi}_0, \bar{\phi}_i)$ in $\chi^{-1}(s_0) \times \chi^{-1}(s_i)$ such that $\triangle_i(\phi_0, \phi_i) = \triangle_i(\bar{\phi}_0, \bar{\phi}_i)$. Then, $\phi_0 \circ \psi_L \circ \phi_i^{\Gamma_i(x,e)} = \bar{\phi}_0 \circ \psi_L \circ \bar{\phi}_i^{\Gamma_i(x,e)}$ and $\phi_0 \circ \psi_L \circ \phi_i^{\Gamma_i(x^*,e^*)} = \bar{\phi}_0 \circ \psi_L \circ \bar{\phi}_i^{\Gamma_i(x^*,e^*)}$. Combining these two equalities, we obtain

$$\phi_i^{\Gamma_i(x^*,e^*) - \Gamma_i(x,e)} = \bar{\phi}_i^{\Gamma_i(x^*,e^*) - \Gamma_i(x,e)},$$

that leads to $\phi_i = \bar{\phi}_i$ and then to $\phi_0 = \bar{\phi}_0$.[6] Thus, $\triangle_i$ is injective.

Then, as $\chi^{-1}(s_0) \times \chi^{-1}(s_i)$ and $\chi^{-1}(s) \times \chi^{-1}(s^*)$ have the same (finite) cardinality, $\triangle_i$ is a bijection. So, if (ϕ_0, ϕ_i) is chosen uniformly at random in $\chi^{-1}(s_0) \times \chi^{-1}(s_i)$ then (ϕ, ϕ^*) is uniformly distributed on $\chi^{-1}(s) \times \chi^{-1}(s^*)$, for any choice of ϕ_j, $j = 1, \dots, i-1, i+1, \dots, n$. Then, the same occurs when the whole tuple $\hat{\phi}$ is chosen uniformly at random in $\hat{\chi}^{-1}(\hat{s})$. Consequently, ϕ and ϕ^* are independent uniformly distributed random variables. In particular, this independence implies that the knowledge of $\Phi_{\hat{k}}(x^*, e^*) = \phi^*(x^*)$ does not affect the probability distribution of $\Phi_{\hat{k}}(x, e) = \phi(x)$. Thus, by Lemma 3, $\Phi_{\hat{k}}(x, e)$ is uniformly distributed on a set of size $|[x]|$. Then, $\hat{\mathbf{H}}$ is $1/p$-universal$_2$. $\square$

[6] Note that, as $|\Gamma_i(x^*, e^*) - \Gamma_i(x, e)| < q$, we have $\gcd(\Gamma_i(x^*, e^*) - \Gamma_i(x, e), |H|) = 1$. So there are $a, b \in \{0, \dots, |H|-1\}$ such that $a(\Gamma_i(x^*, e^*) - \Gamma_i(x, e)) = 1 + b|H|$, and, consequently, $\phi_i^{a(\Gamma_i(x^*,e^*) - \Gamma_i(x,e))} = \phi_i^{1+b|H|} = \phi_i$.