A Group-Theoretic Approach for the Construction of Secure Cryptographic Primitives

[1]Odule, T.J. & [2]Awodele, O.
[1]Department of Mathematical Sciences, Olabisi Onabanjo University, P.M.B. 2002 Ago-Iwoye, Nigeria
[2]Department of Computer Science, Babcock University, Ilishan Remo, Nigeria.
E-mail: [1]tola.odule@oouagoiwoye.edu.ng; [2]awodeleo@babcock.edu.ng

Abstract

This paper generalizes the theory of universal hashing in the construction of cryptographic protocols using group-theoretic language formalisms. This idea is due to Wegman and Carter who gave a construction in 1981 which is extremely useful when the number of authenticators is small compared to the number of possible source states (plaintext messages) in order to accommodate the situation where we would like to authenticate a sequence of messages with the same key. Unlike previous methods for doing this we do not require that each message in the sequence have a “counter” attached to it. We provide necessary definitions and theory and then give a construction which achieves our goals.

Keywords: Universal hashing, projective hash family, cryptographic protocol, group-theoretic language,

1. INTRODUCTION

The philosophy behind a universal one-way hash function (UOWHF) is that if, first the input is selected and subsequently the hash function, it does not help an opponent to find collisions for the hash function [1]. Collisions are only useful if first the function is fixed and subsequently one can search for two colliding inputs.

This definition was generalized in [2], where a UOWHF is defined as a three party game with an initial string supplier *S,* a hash function instance generator *G* and a collision string finder *F.* are probabilistic polynomial time algorithms. The game consists of three moves:

1. *S* outputs an initial string x $\in \sum^n$ and sends it to both *G* and *F.*
2. *G* chooses an $h \in {}_R H_n$ independently of *x* and sends it to *F.*
3. *F* outputs either “?” or an $x' \in \sum^n$ such that $h(x') = h(x)$.

F wins the game if its output is not equal to “?”. The input *x* is selected by *S* according to a certain distribution. In the most general case this is the collection of all ensembles with length *n.* If a different ensemble is introduced, a different definition is obtained. In the original definition of [3] the initial string supplier and the collision string finder were the same algorithm, which imposes the unnecessary restriction that *x* should be selected according to all polynomially samplable ensembles (the collision string finder has to be a polynomial time algorithm).

The construction by M. Naor and M. Yung [4] also satisfied this more general definition. On the other hand their definition is less complicated: in fact it does not really make sense for *S* to send *x* to *G*, as *G* chooses subsequently *h* independent from *x.* In [2, 5] the hierarchy between different types of UOWHF has been studied.

2. PRELIMINARIES

We recall some basic terminology and notation.

A function $f(\ell)$ mapping non-negative integers to non-negative reals is called negligible (*in* ℓ) if for all $c \geq 1$, there exists $\ell_0 > 0$ such that $f(\ell) \leq 1/\ell^c$ for all $\ell \geq \ell_0$.

Let *X* and *Y* be random variables taking values in a finite set *S.* The statistical distance between *X* and *Y* is defined to be

$$Dist\,(X,Y) = \frac{1}{2}\sum_{s\in S}|\Pr[X=s]-\Pr[Y=s]|$$

Equivalently,

$$Dist\ (X,Y) = \frac{1}{2}\max_{S \subset S}|\Pr[X \in S'] - \Pr[Y \in S']|$$

We shall say that X and Y are ∈ -close if $Dist(X, Y) \leq \in$.

Let $\mathbf{X} = (X_\ell)_{\ell \geq 0}$ and $\mathbf{Y} = (Y_\ell)_{\ell \geq 0}$ be sequences of random variables, where for each $\ell \geq 0$, X_ℓ and Y_ℓ take values in a finite set S_ℓ. Then we say that **X** and **Y** are *statistically indistinguishable* if *Dist* (X_ℓ, Y_ℓ) is a negligible function in ℓ. For computational purposes, we will generally work in a setting where the sets S_ℓ can be encoded as bit strings whose length is polynomial in ℓ. for any probabilistic algorithm A that outputs o or 1, we define the *distinguishing advantage for* A (with respect to X and Y) as the function

$$Dist\ X,\ Y(\ell) = \left|\Pr[A(1^\ell, X_\ell) = 1] - \Pr[A(1^\ell, Y_\ell) = 1]\right|$$

Here, the notation 1^ℓ denotes the unary encoding of ℓ as a sequence of ℓ copies of 1, and the probability is with respect of the random coin tosses of the algorithm A and the distributions of X_ℓ and Y_ℓ. We say that **X** and **Y** are *computationally indistinguishable* if for all probabilistic, polynomial-time A, the function $Dist\ X,\ Y\ (\ell)$ in negligible in ℓ.

For a positive integer Z, Z_N denotes the ring of integers module N, and Z^*_N denotes the corresponding multiplicative group of units. For $a \in Z$, (a mod N) $\in Z_N$ denotes the residue class of a modulo N.
For an element g of a group G, (g) denotes the subgroup of G generated by g. Likewise, for a subset U of G, (U) denotes the subgroup of G generated by U.

2.1 Universal Hashing

Before defining universal projective hash functions, we recall some definitions relating to the classical notion of "universal hashing" [6, 7].

Let X and Π be finite, non-empty sets. Let $H = (H_k)_{k \in K}$ be a collection of functions indexed by K, so that for every $k \in K$, H_k is a function from X into Π.
Note that we may have $H_k = H_k$ for $k \neq k'$. We call $\mathbf{F} = (H, K, X, \Pi)$ a hash family, and each H_k a hash function.

Definition 1: Let $\mathbf{F} = (H, K, X, \Pi)$ be a hash family, and consider the probability space defined by choosing $k \in$ K at random. We call **F** pair-wise independent if for all $x, x^* \in X$ with $x \neq x^*$, it holds that $H_k\ (x)$ and $H_k\ (x^*)$ are uniformly and independently distributed over Π.

Note that there are many well-known, and very simple constructions of pair-wise independent hash families.

2.2 Universal Projective Hashing

We now introduce the concept of universal projective hashing. Let $\mathbf{F} = (H, K, X, \Pi)$ be a hash family. Let L be a non-empty, proper subset of X**.** Let S be a finite, non-empty set, and let $a : K \rightarrow S$ be a function. Set **H** (H, K, X, L, Π, S, a).

Definition 2: $\mathbf{H} = (H, K, X, L, \Pi, S, a)$, defined as above, is called a *projective hash family* (for (X, L)) if for all $k \in K$, the action of H_k on L is determined by $a\ (k)$.

In other words, for all $k \in K$, the value $a(k)$ "encodes" the action of H_k on L (and possibly more than that), so that given $a\ (k)$ and $x \in$ L, the value $H_k\ (x)$ is uniquely determined.

Definition 3: Let $\mathbf{H} = (H, K, X, L, \Pi, S, a)$ be a projective hash family, and let $\varepsilon \geq 0$ be a real number. Consider the probability space defined by choosing $k \in K$ at random. We say that **H** is ε-*universal* if for all $s \in S$, $x \in X \backslash L$, and $\pi \in \Pi$, it holds that:

$\Pr[H_k\ (x) = \pi \wedge a\ (k) = s] \leq \varepsilon \Pr\ [a(k) = s]$

We say that **H** is ε – *universal*$_2$ if for all s ∈ S, x, x* $\in X$ and $\pi, \pi^* \in \Pi$ with $x \notin L\ U\ \{x^*\}$, it holds that:

$\Pr[H_k\ (x) = \pi \wedge H_k\ \ (x^*) = \pi^* \wedge a(k) = s] \leq \varepsilon \Pr[H_k\ \ (x^*) = \pi^* \wedge a(k) = s]$

We will sometimes refer to the value of **H** in the above definition as the *error rate* of **H.**

Note that if **H** is ε – *universal*$_2$**,** then it is also ε – *universal* (note that $|X| \geq 2$).

Interpretation We can reformulate the above definition as follows. Let **H** = (H, K, X, L, Π, S, a) be a projective hash family, and consider the probability space defined by choosing $k \in K$ at random. **H** is ε – *universal* means that conditioned on a fixed value of $a(k)$, even though the value of H_k is completely determined on L, for any $x \in X \backslash L$, the value of $H_k(x)$ can be guessed with probability at most ε. **H** is ε – *universal₂* means that in addition, for any $x^* \in X \backslash L$, conditioned on fixed values of $a(k)$ and $H_k(x^*)$, for any $x \in X \backslash L$ with $x \neq x^*$, the value of $H_k(x)$ can be guessed with probability at most ε.

2.2.1 Justification

We now discuss the justification for *Definition 3.* Let **H** be a projective hash family, and consider the following game played by an adversary.

At the beginning of the game, $k \in K$ is chosen at random, and the adversary is given $s= a(k)$. Initially, the adversary has no other information about k, but during the course of the game, he is allowed to make a sequence of oracle queries to learn more about k.

There are two types of oracle queries [8,9]. One type of oracle query is a *test query:* the adversary submits $x \in X$ and $\pi \in \Pi$ to the oracle, and the oracle tells the adversary whether or not $H_k(x) = \pi$ The other type of oracle query is an *evaluation query:* the adversary submits $x^* \in X$ to the oracle, and the oracle tells the adversary the value $\pi^* = H_k(x^*)$.

During the course of the game, the adversary is allowed to make an arbitrary number of *test queries,* but only one *evaluation query.* Moreover, after the evaluation query, he is not allowed to submit (x^*, π^*) to the oracle in any subsequent test queries. We say the adversary wins the game if he submits a test query (x, π) with $x \in X \backslash L$ and $H_k(x) = \pi$.

The completes the description of the game. Note that in this game, the adversary's strategy is quite arbitrary, and need not be efficiently computable. Moreover, the strategy may be adaptive, in the sense that an oracle query made by the adversary may depend in an arbitrary way on all information available to the adversary at that time.

It is easy to see from the definition that if **H** is ε – *universal₂,* then regardless of the adversary's strategy, he wins the game with probability at most $Q.\varepsilon$, where Q is a bound on the number of test queries made by the adversary. Note that while this property is a consequence of the definition of ε – *universal₂*, it is not necessarily equivalent to the definition of ε – *universal₂*. In fact, this property suffices to prove the main results of this paper, and indeed, all we need is this property in the case where x^* is chosen at random from $X \backslash L$, and where the adversary is computationally bounded.

2.2.2 From universal projective to universal₂ projective

Let **H** = *(H, K, X, L, Π, S, a) be an* ε – universal projective hash family. The next construction turns **H** into an ε – *universal₂* projective hash family **H⁺** for ($X \backslash L$). Let us assume that we have injective functions $\Gamma: X \rightarrow \{0,1\}^n$ and $\Gamma': \Pi \rightarrow \{0,1\}^n$ for some appropriately large positive integers n and n'.

Let $\mathbf{H}^+ = (\mathbf{H}^+, K^{2n}, X, L, \{0,1\}^{n'}, S^{2n}, a^+)$, where **H⁺** and a^+ are defined as follows.

For $k = (k_{1,0}, k_{1,1} \ldots, k_{n,0}, k_{n,1}) \in K^{2n}$ and $x \in X$ with $\Gamma(x) = (\gamma_1, \ldots, \gamma_n) \in \{0,1\}^n$, we define.

$$H^{\frac{1}{k}}(x) \hbar \bigoplus_{i=1}^{n} \Gamma'(H_k(x))$$

and

$$a^+(k) = (a(k_{1,0}), a(k_{1,1}), \ldots, a(k_{n,0}), a(k_{n,1}))$$

Here, "$\oplus$" denotes the bit-wise "exclusion" or operation on n'–bit strings.

Lemma 1: Let **H** and **H'** be as defined in the above construction. If **H** is an ε – universal projective hash family, then **H⁺** is an ε-*universal₂* projective hash family.

Proof: It is immediate that *Definition 2* is satisfied.

The proof that *Definition 3* is satisfied follows from a simple "conditioning argument", the details of which we now provide.
Consider the probability space defined by choosing $k \in K^{2n}$ at random. To show that **H⁺** is ε – *universal₂,* we have to show that for any $x, x^* \in X$ with $x \notin L \cup \{x^*\}$, conditioned on any fixed values of $H^{\frac{+}{k}}(x)$ and $a^+(k)$, and value of $H^{\frac{+}{k}}(x)$ can be guessed with probability at most ε.

Let $\Gamma(x) = (\gamma_1, \ldots, \gamma_n) \in \{0,1\}^n$ and $\Gamma(x^*) = (\gamma^*_1, \ldots, \gamma^*_n) \in \{0,1\}^n$. Since $x \neq x^*$, we must have $\gamma_1 \neq \gamma^*_1$ for some $1 \leq i \leq n$, and without loss of generality, let us assume that $i = n$.

In addition to conditioning on fixed values of $H\frac{+}{k}(x)$ and $a^{+}(k)$, let us further condition on fixed values of $K_{1,0}$, $K_{1,1}$, …, $K_{n\text{-}1.0}$, $K_{n\text{-}1.1}$, as we as $k_{n.\gamma n*}$ (consistent with the fixed values of $H\frac{+}{k}(x)$ and $a^{+}(k)$. in this conditional probability space, the value of $H\frac{+}{k}(x)$ determines the value of $H_{kn.m}$ (x) and thus, if the value of $H\frac{+}{k}(x)$ could be guessed with probability greater than ε, then so could the value of $H_{kn.m}$ (x). But since **H** is ε – universal, it follows that the value of $H_{kn.m}$ (x) cannot be guessed with probability greater than ε . We conclude that value of $H\frac{+}{k}(x)$ cannot be guessed with probability greater than ε in this conditional probability space. Since this holds for all fixed values of $k_{1,0}$, $k_{1,1}$, …, $k_{n\text{-}1.0}$, $k_{n\text{-}1.1}$, and $k_{n.\gamma n*}$ under consideration, it holds as well in the conditional probability space where just $H\frac{+}{k}(x)$ and $a^{+}(k)$ are fixed. Which proves the theorem.

The following construction is a variation on *Lemma 2*. It extends the sets *X* and *L* by taking the Cartesian product of these sets with a fixed, finite set *E*. Such extensions will prove useful in the sequel.

Let **H** = *(H, K, X, L, Π, S, a)* be an ε – universal projective hash family. Let *E* be a non-empty, finite set.

Let us assume that we have injective functions Γ : *X* x *E* →{0,1}“ and Γ’:Π → {0,1}” for some appropriately large positive integers *n* and *n’*. Let $\mathbf{H}^{\updownarrow}$ = ($\mathrm{H}^{\updownarrow}$, K^{2n}, *X* x *E*, *L* x *E*, {0,1}” , S^{2n} , $a^{\updownarrow}$), where $H^{\updownarrow}$ and $a^{\updownarrow}$ are defined as follows.
For $k = (k_{1,0}, K_{1,1}, \ldots, K_{n.0}, K_{n.1}) \in k^{2n}$, and (*x, e*) ∈ *X* x *E* with $\Gamma(x,e) = (\gamma_1, \ldots, \gamma_n) \in$ {0,1}”, we define

$$H_k^{\updownarrow}(x,e) = \bigoplus_{i=1}^{n} \Gamma'(H_{ki,yi}(x))$$

$$a^{\updownarrow}(k) = (a(k_{1,0}), a(k_{1.1}), \ldots, a(k_{n.0}), a(k_{n.1}))$$

The proof of the following lemma is essentially the same as the proof of *Lemma 2.*

Lemma 2: Let **H** and $\mathbf{H}^{\updownarrow}$ be as defined in the above construction. If **H** is an ε – universal projective hash family, then $\mathbf{H}^{\updownarrow}$ is an ε – *universal*$_2$ projective hash family.

3.0 UNIVERSAL PROJECTIVE HASH FAMILIES: CONSTRUCTIONS

We now present group-theoretic constructions of universal projective hash families.

3.1 Diverse Group Systems And Derived Projective Hash Families

Let *X, L* and Π be finite abelian groups, where *L* is a proper subgroup of *X*. We will use additive notation for these groups.
Let Hom(*X*, Π) denote the group of all homomorphisms ϕ:*X* → Π. This is also a finite abelian group for which we use additive notation as well. For ϕ,ϕ' ∈ Hom(*X*, Π), *x* ∈ *X*, and *a* ∈ *Z*, we have $(\phi + \phi')(x) = \phi(x) + \phi'(x)$, $(\phi - \phi)(x) = \phi(x) - \phi'(x)$, and $a\phi(x) = \phi(ax)$. The zero element of Hom(*X*, Π) sends all elements of *X* to 0 ∈ Π.

Definition 4 Let *X, L,* Π be as above. Let *H* be a subgroup of Hom(*X*, Π). We call **G** = (*H, X, L,* Π) a group system.
Let **G** = (*H, X, L,* Π) be a group system, and let $g_1, \ldots, g_d \in L$ be a set of generators for *L* . Let **H** = (*H, K, X, L,* Π*, S, a)*, where

- for randomly chosen *k* ∈ *K*, H_k is uniformly distributed over *H* **,**
- $S = \Pi^d$, and
- the map *a* : *K* → *S* sends *k* ∈ *K* to $(\phi(g_1), \ldots, \phi(g_d)) \in S$, where $\phi = H_k$.

It is easy seen that **H** is a projective hash family. To see this, note that if *x* ∈ *L*, then there exist $w_1, \ldots, w_d \in Z$ such that $x = \sum_{i=1}^{d} w_i\, g_i$; now, for *k* ∈ *K* with $H_k = \emptyset$ and $a(k) = (\mu_i, \ldots, \mu_d)$, we have

$$H_k(x) = \emptyset(\sum_{i=1}^{d} w_i\, g_i) = \sum_{i=1}^{d} w_i\, \emptyset(g_i) = \sum_{i=1}^{d} w_i\, \mu_i \ (\mathrm{x})$$

Thus, the action of H_k on *L* is determined by *a*(*k*), as required.

Definition 5 Let **G** be a group system as above and let **H** be a projective hash family as above. Then we say that **H** is a projective hash family derived from **G.**

Looking ahead, we remark that the reason for defining *a* in this way is to facilitate efficient implementation of the public evaluation algorithm for a hash proof system with which **H** may be associated. In this context, if a “witness” for *x* is $w_1, \ldots, w_d$, assuming arithmetic in Π is efficiently implemented.

Our first goal is to investigate the conditions under which a projective hash family derived from a group system is ε – *universal* for some ε < 1.

Definition 6 Let **G** = (H, H, L, Π) be a group system. We say that **G** is diverse if for all $x \in X \setminus L$, there exists Ø ∈ H such that Ø(L) = ⟨0⟩, but Ø(x) ≠ 0.
It is not difficult to see that diversity is a necessary condition for a group system if any derived projective hash family is to be *ε – universal* for some ε < 1. We will show in *Theorem 1* below that any projective hash family derived from a diverse group system is *ε – universal*, where ε = 1/ $\tilde{p}$ and $\tilde{p}$ is the smallest prime dividing $|X/L|$.

3.2 A Universal Projective Hash Family

Throughout this section, **G** = (H , X, L, Π) denotes a group system, **H** = (H, K, X, L, Π, S, a) denotes a projective hash family derived from **G**, and $\tilde{p}$ denotes the smallest prime dividing $|X/L|$.

Definition 7 For a set Y ⊂ X let us define A(Y) to be the set of Ø ∈ H such that Ø(x) = 0 for all x ∈ Y ; that is, A(Y) is the collection of homomorphisms in H that annihilate Y.
It is clear that A(Y) is a subgroup of H , and that A(Y) = (⟨Y⟩). The following is a straightforward re-statement of *Definition 6.*

Lemma 3 **G** is diverse if and only if for all $x \in X|L$, A(L) A(L {x}) is a proper subgroup of A(L). ∪

Lemma 4 If p is a prime dividing |A(L)|, then p divides $|X/L|$.
Proof. Let p be a prime dividing |A(L)|. Then there exists an element Ø ∈ A(L) of order p. Let a = $|X/L|$, and note that for all x ∈ X, we must have $ax \in L$, since a is the order of the factor group X/L. Therefore, for all $x \in X$, we have (a – Ø)(x) = Ø (ax) = 0 , the latter equality holding since Ø annihilates L and $ax \in L$. It follows that p divides a.

Definition 8 For $x \in X$, let $\mathcal{E}_x : H \rightarrow$ Π E be the map that sends Ø ∈ H to Ø(x) ∈ Π. Let us also define T (x) = $\mathcal{E}_x$ (A(L)).

Clearly, $\mathcal{E}_x$ is a group homomorphism, and T (x) is a subgroup of Π.

Lemma 5 If **G** is diverse, then for all $x \in X \setminus$ L , |T (x)| is at least $\tilde{p}$.

Proof Let $x \in X \setminus L$. Consider the restriction of the map $\mathcal{E}_x$ to A(L). The image of this map is T (x), and the kernel is A(L {x}). Therefore, T (x) is isomorphic to the factor group A (L) / A(L {x}). Since **G** is assumed diverse, by *Lemma 3*, A(L {x}) is a proper subgroup of A(L) not equal to 1, and so is divisible by some prime p dividing A(L). By *Lemma 4,* this prime p divides |A(L)|.

∪

Lemma 6 Let $s \in a$ (K)s be fixed. Consider the probability space defined by choosing $k \in a^{-1}$ (s) at random, and let $\rho = H_k$. Then ρ is uniformly distributed over a coset Ψ_s + A(L) of A(L) in H , the precise coset depending on s.

∪

Proof Let $g_1,\ldots, g_d$ be the set of generators defining a . Let $\tilde{a}$: H → S be the map that sends Ø ∈ H to (Ø(g_1),…,Ø(g_d) ∈ S. It is evident that ρ is uniformly distributed over $\tilde{a}^{-1}(s)$. Moreover, $\tilde{a}$ is clearly a group homomorphism with kernel A({g_1,…, g_d}) = A(L). If follows that $\tilde{a}^{-1}(s)$∪ is a coset of A(L) in H .

In *Lemma 6*, there are many choices for the "coset leader" Ψ_s ∈ H ; however, let us fix one such choice arbitrarily, so that for the rest of this section Ψ_s denotes this coset leader.

Theorem 1 Let $s \in a$ (K) and $x \in X$ be fixed. Consider the probability space defined by choosing $k \in a^{-1}$ (s) at random, and let $\pi = H_k$ (x). Then π is uniformly distributed over a coset of T (x) in Π_ (the precise coset depending on s and x). In particular, if **G** is diverse, then **H** is 1/ $\tilde{p}$ – *universal.*

Proof Let $\rho = H_k$. By *Lemma 6*, ρ is uniformly distributed over Ψ, + A(L). Since $\pi = \rho(x)$, it follows that π is uniformly distributed over $\mathcal{E}_x$ (Ψ_s + A(L)) = Ψ_s (x) + T (x). That proves the first statement of the theorem. The second statement follows immediately from *Lemma 5,* and the fact that |Ψ_s (x) + T (x)| = |T (x)|.

3.3 A Universal₂ Projective Hash Family

We continue with the notation established in section 3.2. In particular, **G** = (H, X, L, Π) denotes a group system, **H** = (H, K, X, L, Π, S, a) denotes a projective hash family derived from **G,** and $\tilde{p}$ denotes the smallest prime dividing $|X \setminus L|$.

Starting with **H,** and applying the construction of *Lemma 1* or *Lemma 2*, we can obtain a *universal$_2$* projective hash family. However, by exploiting the group structure underlying **H**, we can construct a more efficient *universal$_2$* projective hash family $\hat{H}$.

Let E be an arbitrary finite set. $\hat{\boldsymbol{H}}$ is to be a projective hash family for (X x E, L x E). Fix an injective encoding function Γ: X x E → {0,…, $\tilde{p}$ - 1}^{n} ; where n is sufficiently large. Let $\hat{\boldsymbol{H}}$ = ($\hat{H}$, K^{n+1}, X x E, L x E, Π, S^{n+1}, $\hat{a}$), where $\hat{H}$ and $\hat{a}$ are defined as follows. For $\vec{k}$ = (k', k_1 ,…, k_n) ∈ K^{n+1} , $x \in X$, and e ∈ E, we define.

$$\hat{H}_{\vec{k}}\,(x,e) = K_{k'}\,(x) + \sum_{i=1}^{d} \gamma_i H_{K_i}\,(x) \text{ where } (\gamma_i\,, \ldots, \gamma_n) = \Gamma(x,e),$$

and we define $\hat{a}(k) = (a(k'), a(k_1) ,\ldots, a(k_n))$:

It is clear that $\hat{\boldsymbol{H}}$ is a projective hash family.

Theorem 2 Let $\hat{\boldsymbol{H}}$ be as above. Let $\vec{s}$ ∈ a $(K)^{n+1}$, x, x^* ∈ X , and e, e^* ∈ E be fixed**,** where (x, e) ≠ (x^* , e*)**.** Consider the probability space defined by choosing $k \in a^{-1}$ **(*s*)** at random, and let π = $\hat{H}_{\vec{k}}$ (x, e) and π^* = $\hat{H}_{\vec{k}}$ (x^* , e^*). Then π is uniformly distributed over a coset of T (x) in Π _ (the precise coset depending on s, x and e), and π^* is uniformly and independently distributed over a coset of T (x^*) in Π _ (the precise coset depending on s, x^* and e^*). In particular, if the underlying group system **G** is diverse, then $\hat{\mathbf{H}}$ is 1/ $\tilde{p}$ – *universal*$_2$**.**

Before proving this theorem, we state another elementary lemma.

Let $M \in Z^{axb}$ be an integer matrix with a rows and b columns. Let G be a finite abelian group. Let **T** (M , G) : $G^h \rightarrow G^a$ be the map that sends $\vec{u} \in G^h$ to $\vec{v} \in G^a$, where $\vec{v}^{\,\gamma} = \mathrm{M}\vec{u}^{\,\gamma}$;
here, (…)$^\gamma$ denotes transposition. Clearly, **T**(M, G) is a group homomorphism.

Lemma 7 Let M and G be as above. If for all primes p dividing |G|, the rows of M are linearly independent *modulo p*, then **T** (M ,G) is subjective.

Proof The proof is by basic linear algebra, and we include it for completeness.

Let $\prod_{i=1}^{r} p_i^{c_i}$ be the prime factorization of $|\mathcal{G}|$. From the conditions of the lemma, it follows that for each 1 ≤ i ≤ r there is a square sub-matrix M_i , consisting of a columns of M , that is invertible over Z_{pi} and, therefore, also over $Z_{p_i}^{c_i}$. Hence, for each 1≤ i ≤ r there is a matrix $N_i \in \mathrm{Z}^{\mathrm{bxa}}$ such that M . $N_i \equiv I \pmod{p_i^{c_i}}$, where I is the a x a identify matrix over Z. Combining N_1,… N_r using *Chinese Remainder Theorem,* there is a matrix $N \in Z^{bxa}$ such that M . $N \equiv I$ (mod |G|). Hence, for all $v' \in G^a$, we have $v^{\gamma} = Mu^{'\gamma}$, where $u^{'\gamma} = N\,v^{'\gamma}$.

Proof of Theorem 2. Let $\vec{s}$ = (s', s_1,…,s_n), (γ_1,…, γ_n) = Γ (x,e), and (γ_1^*,…, γ_n^*) = Γ (x^* , e^*). Let (ρ', ρ_1,…, ρ_n) = ($H_{k'}$, H_{k_1} ,…, H_{k_n}). Now define the matrix $M \in Z^{2\mathrm{x(n+1)}}$ as

$$M = \begin{pmatrix} 1 & \gamma_1 & \gamma_2 & \cdots & \gamma_n \\ 1 & \gamma_1^* & \gamma_2^* & \cdots & \gamma_n^* \end{pmatrix};$$

so that if

$$(\vec{\rho}, \vec{\rho}^{\,*})^{\gamma} = M\,(\rho', \rho_1, \ldots, \rho_n)^{\gamma}$$

then we have (π, π^*) = ($\rho(x)$, ρ^* (x^*)).

By the definition of Γ , and by *Lemma* 4, we see that ((γ_1 ,…, γ_n) and (($\gamma_1^*, \ldots, \gamma_n^*$) are distinct modulo any prime p that divides $A(L)$. Therefore, *Lemma 7* implies that the map **T**(M, A)) is surjective. By *Lemma 6,* (ρ', ρ_1,…, ρ_n) is uniformly distributed over ($\Psi_{s'} + A(L)$, $\Psi_{s_{11}} + A(L)$,…, $\Psi_{s_n} + A(L)$) ;

Thus, ($\vec{\rho}$, $\vec{\rho}^{\,*}$) is uniformly distributed over ($\vec{\Psi} + A(I)$, $\vec{\Psi}^* + A(I)$) , where Ψ, $\vec{\Psi}^*)^{\gamma} = M$ ($\Psi_{s'}$, Ψ_{s_1} ,…, Ψ_{s_n})$^{\gamma}$. If follows that (π, π^*) is uniformly distributed over ($\vec{\Psi}$ (x) + T (x), Ψ^* (x^*) + T (x^*)).
That proves the first statement of the theorem. The second statement now follows from *Lemma 5.*

If $\tilde{\rho}$ is small, then *Lemma 1* can be used to reduce the error to at most $1/\tilde{\rho}^1$ for a suitable value of t. However, this comes at the cost of a *multiplicative* factor t in efficiency. We now describe another construction that achieves an error rate of $1/\tilde{\rho}^1$ that comes at the cost of just an *additive* factor of *O(t)* in efficiency.

Let $t \geq 1$ be fixed, and let E be an arbitrary finite set. Our construction yields a projective hash family $\hat{\mathbf{H}}$ for (X x E, L x E). We use the same name $\hat{\mathbf{H}}$ for this projective hash family as in the construction of *Theorem 2,* because when $t = 1$, the constructions are identical. Fix an injective encoding function.

$$\Gamma : X \text{ x } E \to \{0,\ldots, p-1\}^{\text{n}};$$

when n is sufficiently large.

Let $\hat{\mathbf{H}} = (\hat{\mathrm{H}}, K^{n+21=1}, X \text{ x } E, L \text{ x } E, \Pi, S^{n+21=1}, \hat{a})$, where $\hat{H}$ and $\hat{a}$ are defined as follows. For

$\vec{k} = (k'_1,\ldots,k'_1, k'_1,\ldots, K_{n+21=1}) \in K^{n+21=1}$; $x \in X$, and $e \in E$, we define

$$\hat{\mathrm{H}}_{\vec{k}}(x, e) = (\pi_1, \ldots \pi_t), \text{where } \pi_j = H_{k'_j}(x) + \sum_{i=1}^{d} \gamma_i H_{k_{i+j-1}}(x) \quad (j = 1, \ldots, t),$$

and $(\gamma_1, \ldots, \gamma_n) = \Gamma(x, e)$. We also define

$$\hat{a}(\vec{k}) = (a(k'_j),\ldots, a(k'_j), a(k_1),\ldots, a(k_{n+t-1})).$$

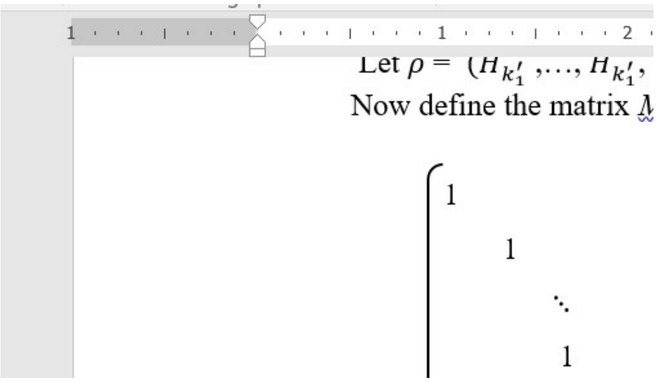
Again, it is clear that $\hat{\mathbf{H}}$ is a projective hash family.

Theorem 3 Let $\hat{\mathbf{H}}$ be as above. Let $\vec{s} \in a\,(K)^{n+2t-1}$, $x, x^* \in X$, and $e, e^* \in E$ be fixed, where $(x, e) \neq (x^*, e)$. Consider the probability space defined by choosing $\vec{k} \in \hat{a}^{-1}(\vec{s})$ at random, and let $\vec{\pi} = \hat{H}_{\vec{k}}(x, e)$ and $\vec{\pi}^* = \hat{H}_{\vec{k}}(x^*, e^*)$. Then $\vec{\pi}$ is uniformly distributed over a coset of $T(x)$' in Π' (the precise coset depending on s, x, and e), and $\vec{\pi}^*$ is uniformly and independently distributed over a coset of $T(x^*)$' in Π' (the precise coset depending on s, x^*, and e^*). In particular, if the underlying group system **G** is diverse, then **H** is $1 / \tilde{p}$ – *universal*$_2$.

Proof Let $(\gamma_1,\ldots, \gamma_n) = \Gamma(x,e)$, and $(\gamma_1^*, \ldots, \gamma_n^*) = \Gamma(x,e)$

Let $\vec{\rho} = (H_{k'_1},\ldots, H_{k'_1}, H_{k_1},\ldots, H_{k_n+t-1}) \in H^{n+2t-1}$.

Now define the matrix $M \in Z^{2tx(n+2t-1)}$ as



Let $\rho = (H_{k'_1},\ldots, H_{k'_1},$
Now define the matrix M

$$\begin{matrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{matrix}$$

So that if $\vec{\rho}_1,\ldots, \vec{\rho}_1, \vec{\rho}_1^*,\ldots, \vec{\rho}_1^{*\ \tau} = M\,\vec{\rho}^{\tau}$

Then $\vec{\pi} = (\vec{\rho}_1(x),\ldots, \vec{\rho}_t(x))$ and $\vec{\pi}^* = (\vec{\rho}_1^*(x),\ldots, \vec{\rho}_1^*(x))$

Claim: The rows of M are linearly independent modulo p for any prime p dividing $|A(L)|$.
The theorem is implied by the claim, as we now argue. By *Lemma 7,* the map **T**(M, $A(L)$) is surjective. By *Lemma 8*, $\vec{\rho}$ is uniformly distributed over a coset of $A(L)^{n+2t-1}$ in H^{n+2t-1}. If follows that $(\vec{\rho}_1,\ldots, \vec{\rho}_1, \vec{\rho}_1^*,\ldots, \vec{\rho}_1^*)$ is uniformly distributed over a coset of $A(L)^{2t}$ H^{2t}, and therefore, $\vec{\pi}$ and $\vec{\pi}^*$ are uniformly and independently distributed over cosets of $T(x)$' and $T(x^*)$', respectively, in Π'.

The proves the first statement of the theorem. The second statement of the theorem now follows from *Lemma 5.*
So now it remains to prove the above claim. Fix a prime p dividing $|A(L)|$, and for $1 \leq i \leq n$ let γ_i and γ_i^* denote the images of γ_i and γ_i^*, respectively, in Z_p, and let M denote the image of M in $Z_p^{2tx(n+2t-1)}$. By the definition of Γ and *Lemma 4*, we know that $\vec{\gamma}_i \neq \vec{\gamma}_i^*$ for some $1 \leq i \leq n$; let i' be the least such i.

Now, suppose that $(c_1,\ldots,c_t, d_1,\ldots, d_{n+t-1}) = (a_1,\ldots,a_t, b_1,\ldots, b_t) \vec{M}$;
for

$$c_1,\ldots,c_t, d_1,\ldots, d_{n+t-1}, = a_1,\ldots,a_t, b_1,\ldots, b_t \in Z_p :$$

Further suppose that $c_1,\ldots,c_t, d_1,\ldots, d_{n+t-1}$ are all zero. To prove the claim, we need to show that $a_1,\ldots,a_t, b_1,\ldots, b_t$ are all zero as well. It is clear from the structure of the matrix M, and since $c_1,\ldots,c_t$ are all zero, that we must have $a_1 = - b_j$ for all $1 \leq j \leq t$. By way of contradiction, suppose that some $a_j \neq 0$ for some $1 \leq j \leq t$, and let j' be the least such j . By direct calculation, one sees that

$$d_{t'+j'-1} = a_{j'} (\vec{\gamma}_{i'} - \vec{\gamma}_{i'}^*) \neq 0.$$

which is a contradiction. That proves the claim.

4.0 MODELS OF DIVERSE GROUP SYSTEMS

In this section, we discuss two model samples of diverse group systems with cryptographic implications.

4.1 Example 1

Let G be a group of prime of prime order q, and let $X = G'$, i.e., X is the direct product of r copies of G. Let L be any proper subgroup of X , and let H = Hom(X, G). Consider the group system **G** = (H , X, L, G).
The group X is isomorphic as a Z_q – vector space to Z_q^r . For the purposes of this discussion, let us simply identify X with Z_q^r and G with Z_q . Under this distribution, L is a proper Z_q - subspace of X . Moreover, H can be identified with the vector space Z_q^r , as follows: for every $v \in Z_q^r$, we define $Ø_v \in H$ to be the map that sends $x \in Z_q^r$ to $(x, v) \in Z_q$, where (.,.) denotes the standard inner product of vectors.

For any set $U \subset Z_q^r$, $A(U)$ is the orthogonal complement in Z_q^r of the subspace of Z_q^r generated by U, Therefore, if U generates of subspace of dimension a, $A(U)$ is a subspace dimension $r – a$.
Now suppose L has dimension d, and that $x \in X \setminus L$. If follows $A(L)$ has dimension $r – d$, and $A(L \quad \{x\}))$ has dimension $r – d – 1$. This shows that **G** is diverse. Moreover, for any $x \in X \setminus L$, we have $T(x) = \mathscr{E}_x (A(L)) = Z_q$. Therefore, a projective hash family derived from **G** is $1/q$ – *universal*, or equivalently, 0-*smooth*.

4.2 Example 2

Let X be a cyclic group of order $a = bb'$, where $b' > 1$ and gcd(b,b') = 1, and let L be the unique subgroup of X of order b. Let H = Hom(X, X), and consider the group system **G** = (H , X, L, X). The group X is isomorphic to Z_a . If we identify X with Z_a , then H can be identified with Z_a as follows: for every $v \in Z_a$, define $Ø_v \in H$ to be the map that sends $x \in Z_a$ to $x.v \in Z_a$.

The group X is of course also isomorphic to Z_b x $Z_{b'}$. If we identify X with Z_b x $Z_{b'}$, then L corresponds to Z_b x $\langle 0 \rangle$. Moreover, we can identify H with Z_b x $Z_{b'}$ as follows: for $(v,v') \in Z_b$ x $Z_{b'}$, let $\Psi_{v,v'} \in H$ be the map that sends $(x,x') \in Z_b$ x $Z_{b'}$ to $(x.v,x'.v') \in Z_b$ x $Z_{b'}$.
Under the identification in the previous paragraph, it is evident that $A(L)$ is the subgroup of H generated by $\Psi_{0,1}$. If we take any $(x, x') \in X \setminus L$, so that $x' \neq 0$, we see that $\Psi_{0,1} (x, x') = (0, x')$. Thus, $\Psi_{0,1} \in A(L \quad \{x, x'\}))$, which shows that **G** is diverse. Therefore, a projective hash family derived from **G** is $1 / \tilde{p}$ – *universal*, where $\tilde{p}$ is the smallest prime dividing b'.
It is also useful to characterize the group $T(x,x') = \mathscr{E}_{x,x'} (A(L))$. Evidently, since $A(L) = \langle \Psi_{0.1} \rangle$, we must have $T(x, x') = \langle 0 \rangle$ x $\langle x' \rangle$.

5. CONCLUSION

In this paper we study the application of universal hashing to the construction oc cryptographic protocols using group-theoretic language formalisms. This idea is due to Wegman and Carter [7] who gave a construction in 1981 which is extremely useful when the number of authenticators is small compared to the number of possible source states (plaintext messages).

The other main contribution of this paper is to generalize the theory of universal hashing in order to accommodate the situation where we would like to authenticate a sequence of message with the same key. Unlike previous methods for doing this we do not require that each message in the sequence have a “counter” attached to it. We provide necessary definitions and theory and then give a construction which achieves our goals.

REFERENCES

[1] Odule, T.J. "International Cryptography and Security of Pubic Hash Functions." Journal of Nigerian Association of Mathematical Physics, vol. 11 pp. 467-474; 2007.

[2] Y. Zheng, T. Matsumoto, and H. Imai, "Connections between several version of one-way hash functions," Proc. SCIS90, The 1990 Symposium on Cryptography and Information Security, Nihondaira, Japan, Jan. 31 – Feb. 2, 1990.

[3] M. Naor and M. Yung, "Universal one-way hash functions and their cryptographic applications," Proc. 21st ACM Symptosium on the Theory of Computing, 1990, pp. 387-394.

[4] M. Naor and M. Yung, Public-key cryptosystems provably secure against chosen ciphertext attacks. In Proc. STOC '90, ACM Press, 1990.

[5] Y, Zheng, T. Matsumoto, and H. Imai, "Structural properties of one-way hash functions," Advances in Cryptology, Proc. Crypto '90 LNCS 537, S. Vanstone, Ed., Springer-Verlag, 1991, pp. 285-302.

[6] J. Carter and M. Wegman. Universal classes of hash functions. Journal of Computer and System Sciences, 18:143{154, 1979}.

[7] M. Wegman and J. Carter. New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences, **22** (1981), pp. 265-279.

[8] M. Bellare and P. Rogaway, Random oracles are practical: a paradigm for designing efficient protocols. In Proc. ACM Computer and Communication Security '93, ACM Press, 1993.

[9] R, Canetti, O. Goldreich, and S. Halevi. The random oracle model, revisied. In Proc. STOC '98, ACM Press, 1998.