A Hybrid Public Key Encryption in Standard Model and A New Intractibility Assumption

Mahabir Prasad Jhanwar and Rana Barua

Stat-Math Unit
Indian Statistical Institute
Kolkata, India

Abstract. We present a hybrid public-key encryption scheme which is provably secure against adaptive chosen ciphertext attack. The scheme is constructed using Kurosawa-Desmedt paradigm [3]. The security of the scheme is based on the Decisional Bilinear Diffie-Hellman problem. We also present a new intractibility assumption for pairing friendly groups. This new assumption is essentially a variant formulation of Decisional Diffie-Hellman(DDH) assumption.
Keywords: IND-CCA2(adaptive chosen ciphertext security), public-key encryption, DDH- Assumption, DBDH-Assumption, Universal Projective Hashing.

1 Introduction

Indistinguishability against adaptive chosen ciphertext attack (IND-CCA2), where an adversary is given the capability to decrypt ciphertexts of his choice, with the exception of a target ciphertext, is considered to be the correct notion of security for general-purpose public-key encryption schemes. In the literature, there are a number of approaches for obtaining public key encryption schemes that are secure under this model. Much of this work, however, has been only achieved with proofs in the random oracle model [5], the most well-known being OAEP [4].

In the standard model, three main techniques have been proposed for constructing CCA-secure encryption schemes. The first approach, by Naor and Yung [6] and subsequently by Dolev, Dwork and Naor [2], builds IND-CCA secure schemes from any chosen-plaintext secure scheme (CPA-secure) and any non-interactive zero knowledge (NIZK) proof system. The resulting schemes, however, are too inefficient for practical use, since they use expensive NIZK proofs.

Cramer and Shoup [7] proposed the first encryption scheme that was simultaneously practical and IND-CCA2 secure in the standard model. Subsequently, Cramer and Shoup [8] generalised their encryption scheme by introducing the notion of hash proof systems (HPS) and gave a framework for constructing IND-CCA2 secure schemes using HPS constructed from a general subset membership problem. They also showed that their scheme can be regarded as a special case of their general construction.

Using a variant of Cramer-Shoup, Kurosawa and Desmedt [3] obtained a very efficient IND-CCA2 secure hybrid encryption scheme. Following Cramer-Shoup, using HPS as a building block, they obtained a new paradigm for constructing hybrid encryption schemes that are secure in the standard model.

Our contribution:

As mentioned above, Kurosawa-Desmedt obtained a new construction of secure hybrid encryption schemes using strongly universal$_2$ projective hash family. Their examples are essentially those of Cramer-Shoup. We give a new construction of a strongly universal$_2$ projective hash family. Consequently, using Kurosawa-Desmedt paradigm [3], from this family we can easily get a hybrid public-key encryption scheme which is secure against adaptive chosen ciphertext attack. The security of the scheme reduces to Decisional Bilinear Diffie-Hellman problem. The underlying security assumptions of the previously constructed hybrid encryption schemes using Kurosawa-Desmedt paradigm are the DDH assumption, Quadratic Residuosity

assumption and Paillier's Decision Composite Residuosity assumption.
Also in this paper we propose a new intractibility assumption for the pairing friendly groups $G, \tilde{G}$ (i.e. there exists a bilinear map $e : G \times G \to \tilde{G}$). Further we show that if the DDH assumption is hard in $\tilde{G}$ then this new assumption is also hard for the groups $G, \tilde{G}$. The known examples for pairing friendly groups are those where G is taken to be the group of points on elliptic curve and $\tilde{G}$ to be a subgroup of multiplicative groups of finite field. One should know that while dealing with elliptic curve cryptography there are examples of reasonably looking cryptographic groups where Diffie-Hellman is known to be as hard as Discrete Logarithm whereas Decision Diffie-Hellman is easy [1]. Further we present a public-key encryption scheme and show it to be secure under this new assumption against indistinguishability(IND) attack.

2 Preliminaries

2.1 Notations and Definitions

Z_q denotes the set of all congruence classes modulo q. $|S|$ denotes the cardinality of S if S is a set. $|n|$ denotes the bit length of n if n is a string or a number. If $A(.,.,..)$ is a probabilistic algorithm, then $A(x_1, x_2, ..) = x$ denotes the experiment of running A on input $x_1, x_2, ..$ and letting x be the outcome. If S is a set, $x \in_R S$ denotes the experiment of choosing $x \in S$ at random.

2.2 Bilinear Groups

We briefly review the necessary facts about the bilinear maps and bilinear maps friendly groups. We use the following notation:

1. G and $\tilde{G}$ are two cyclic groups of prime order q.
2. g is any non zero element of G.
3. e is a bilinear map $e : G \times G \to \tilde{G}$.

We use mulitiplicative notation for group operation in G and $\tilde{G}$. Let G and $\tilde{G}$ be two groups as above. A bilinear map (pairing map) is a map $e : G \times G \to \tilde{G}$ with the following properties.

1. Bilinearity: for all $x, y \in G$ and $a, b \in Z$, we have $e(x^a, y^b) = e(x, y)^{ab}$.
2. Non-degeneracy: $e(g, g) \neq 1$.

we say that G is a bilinear group if the group action in G can be computed efficiently and there exists a group $\tilde{G}$ and an efficiently computable bilinear map $e : G \times G \to \tilde{G}$ as above. Note that the map e is symmetric since $e(g^a, g^b) = e(g, g) = e(g^b, g^a)$.

2.3 Public-Key Encryption Scheme

We recall the definition of a public-key encryption scheme and the notion of security against adaptive chosen ciphertext attack.

A public key encryption scheme provides three algorithms:

KeyGen(l): a probabilistic, polynomial-time key-generation algorithm that on input 1^l, where $l \geq 0$, is a security parameter, outputs a public-key/private-key pair (PK, SK). A public key PK specifies a finite message space M_{PK}.

Encrypt(PK, M): a probabilistic, polynomial-time encryption algorithm that takes as input a public-key PK, 1^l and a message M. It outputs a ciphertext.

Decrypt(SK, C)**:** a polynomial-time decryption algorithm that takes as input a private key SK and a ciphertext C. It outputs a plaintext message or the special symbol reject.

2.4 Adaptive Chosen Ciphertext Security(IND-CCA2)

The strongest and commonly accepted notion of security for a public key encryption system is that of indistinguishability against an adaptive chosen ciphertexts attack. This notion, denoted IND-CCA2, is defined using the following game between a challenger and an adversary $\mathcal{A}$. Both are given the security parameter $l \in Z^+$ as input.

Setup. The challenger runs KeyGen(l) to obtain a random instance of public and private key pair (PK, SK). It gives the public key PK to the adversary.

Query phase 1. The adversary adaptively issues decryption queries C where $C \in \{0,1\}^*$. The challenger responds with Decrypt(SK, C).

Challenge. The adversary outputs two (equal length) messages M_0, M_1. The challenger picks a random $b \in \{0,1\}$ and sets C^*=Encrypt(PK, M_b). It gives C^* to the adversary.

Query Phase 2. The adversary continue to issue decryption queries C as in Phase 1, with the added constraint that $C \neq C^*$. The challenger responds with Decrypt(SK, C).

Guess. Adversary outputs its guess $\hat{b} \in \{0,1\}$ for b and wins the game if $b = \hat{b}$.

The above game is commonly known as the IND-CCA2 game. We define the advantage of $\mathcal{A}$ in this game as $Adv^{\mathcal{A}}_{cca}(l) = |Pr[b = \hat{b}] - \frac{1}{2}|$. An encryption system is (t, q, ϵ)-IND-CCA2 secure if there is no randomized algorithm $\mathcal{A}$ that runs in time t, makes at most q decryption queries, and has advantage at least ϵ in the IND-CCA2 game.

Indistinguishability Attack (IND) In this security model the adversary is not allowed to query the decryption oracle. The security model is essentially the above IND-CCA2 game without Query phase 1 and Query phase 2.

3 Security Assumption

3.1 Decision Diffie-Hellman Assumption (DDH)

The Decision Diffie-Hellman problem in a group G is to distinguish between the distributions (P, P^a, P^b, P^{ab}) and (P, P^a, P^b, P^c) where a, b, c are random in Z^*_q and P is in G. If G happens to be a bilinear group i.e. there exists a bilinear map $e : G \times G \to \tilde{G}$ where $\tilde{G}$ is a group of order q, then Joux and Nguyen [1] point out that DDH in G is easy. To see this, observe that given $P, P^a, P^b, P^c \in G^*$ we have

$$c = ab \bmod q \text{ iff } e(P^a, P^b) = e(P, P^c).$$

As a result one can observe that for most of the existing IND-CCA2 secure public-key encryption schemes which uses pairing maps, the underlying intractibility assumption is that of Decision Bilinear Diffie-Hellman (DBDH). In this article we define a variant formulation of DDH assumption which is hard for bilinear groups. we call this Pairing Decision Diffie-Hellman (PDDH) assumption. Looking at the new assumption one can realise that its not possible to apply the above technique to distinguish the given two distributions.

3.2 Pairing Decision Diffie-Hellman Assumption (PDDH)

Let G be a bilinear group and $e : G \times G \to \tilde{G}$ be a bilinear map, where G and $\tilde{G}$ are groups of prime order q. We use multiplicative notation for group operation in G and $\tilde{G}$. Consider the following two distributions. Let

$$D = \{(\tilde{g}, g_1, g_2, \tilde{g}^r, g_1^r, g_2^r) | r \in Z_q\}$$

$$R = \{(\tilde{g}, g_1, g_2, \tilde{g}^{r_1}, g_1^{r_2}, g_2^{r_2}) | r_1, r_2 \in Z_q, r_1 \neq r_2\}$$

where $\tilde{g} \in \tilde{G}, g_1, g_2 (= g_1^w) \in G$ and $w \in Z_q^*$.
We claim that the above two distributions are indistinguishable. Infact we have the following reduction. If the Decision Diffie-Hellman(DDH) is easy in the group $\tilde{G}$ then Pairing Decision Diffie-Hellman(PDDH) is easy. We can see that given a valid DDH pair

$$\{(\tilde{g}, g_1, g_2, \tilde{g}^r, g_1^r, g_2^r) | r \in Z_q\}$$

one can compute $e(g_1, g_1^r)$ and get the valid DDH tuple

$$\{\tilde{g}, e(g_1, g_1), \tilde{g}^r, e(g_1, g_1)^r\}.$$

3.3 Decisional Bilinear Diffie-Hellman Assumption

Let G be a bilinear group of prime order q. Let $e : G \times G \to \tilde{G}$ be the bilinear map. The decisional bilinear Diffie-Hellman problem in G is as follows:

Given $g, g^a, g^b, g^c \in G$ and $T \in \tilde{G}$, where a, b, c are random elements in Z_q, g is random element in G, T is random element in $\tilde{G}$. We say an algorithm $\mathcal{A}$ that outputs $b \in \{0, 1\}$ has advantage ϵ in solving the DBDH problem in G if

$$|Pr[A(g, g^a, g^b, g^c, e(g, g)^{abc}) = 0] - Pr[(g, g^a, g^b, g^c, T) = 0]| \geq \epsilon$$

We refer to the distribution on the left as **D** and the distribution on the right as **R**.

4 Hash Proof System (HPS)

In this section we review HPS introduced by Cramer and Shoup [8].

Before defining universal hash function, we recall some definitions relating to the classical notion of "universal hashing".

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.

4.1 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 nonempty, proper subset of X. Let S be a finite, nonempty set, and let $\alpha : K \to S$ be a function. Set $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$.

Definition 1
$\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$, 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 $\alpha(k)$ [8].

Definition 2
Let $\mathbf{H} = (H, K, X, L, \Pi, S, \alpha)$ be a projective hash family. Consider the probability space defined by choosing $k \in K$ at random.

Then H is said to be strongly universal$_1$ if for all $s \in S$, $x \in X \backslash L$, and $\pi \in \Pi$, it holds that

$$Pr[H_k(x) = \pi | \alpha(k) = s] = \frac{1}{|\Pi|}.$$

Definition 3([3])

Let **H**=$(H, K, X, L, \Pi, S, \alpha)$ be a projective hash family. Consider the probability space defined by choosing $k \in K$ at random.

Then H is said to be strongly universal$_2$ if for all $s \in S$, $x \in X \backslash L$, and $\pi \in \Pi$, it holds that

$$Pr[H_k(x) = \pi | \alpha(k) = s] = \frac{1}{|\Pi|}$$

and for all $s \in S$, $x, x^* \in X \backslash L$ with $x \neq x^*$, and $\pi, \pi^* \in \Pi$ it holds that

$$Pr[H_k(x) = \pi | H_k(x^*) = \pi^* \wedge \alpha(k) = s] = \frac{1}{|\Pi|}$$

4.2 Diverse Group System

Let X, L and Π be finite abelian groups, L be a proper subgroup of X.

Let $\mathrm{Hom}(X, \Pi)$ denote the group of all homomorphisms $\phi : X \to \Pi$. This is also a finite abelian group. If we use additive notation for the group operation in X, L and Π then the group operation in $\mathrm{Hom}(X, \Pi)$ is as follows. For $\phi, \phi' \in \mathrm{Hom}(X, \Pi)$, $x \in X$, and $\alpha \in Z$, we have $(\phi + \phi')(x) = \phi(x) + \phi'(x), (\phi - \phi')(x) = \phi(x) - \phi'(x)$, and $(a\phi)(x) = a\phi(x) = \phi(ax)$. The zero element of $\mathrm{Hom}(X, \Pi)$ sends all elements of X to $0 \in \Pi$.

Definition 4

Let X, L, Π be as above . Let H be a subgroup of $\mathrm{Hom}(X, \Pi)$. Then **G**=(H, X, L, Π) is called a group system.

Definition 5

Let **G**=(H, X, L, Π) be a group system. We say that **G** is diverse if for all $x \in X \backslash L$, there exists $\phi \in H$ such that $\phi(L) =< 0 >$, i.e. ϕ vanishes on L but $\phi(x) \neq 0$.

4.3 Subset-Membership Problem (SMP)

A subset membership problem SMP specifies a collection $\{instance_n\}_{n \in N}$ such that for every n, $instance_n$ is a probability distribution over problem instance Λ. Each Λ specifies the following:

Non-empty sets, X, L and W such that L is a proper subset of X.

A binary relation $R \subset X \times W$ such that $x \in L$ iff $(x, w) \in R$ for some witness $w \in W$

SMP require that the following Probabilistic polynomial time algorithms exist.

1. Instance sampling: samples an instance Λ according to $instance_n$ on system parameter1^n.
2. Subset sampling: outputs a random $x \in L$ together with a witness $w \in W$ for x on input 1^n and $\Lambda[X, L, W, R]$.
3. Element sampling: outputs a random $x \in X$.

The SMP is said to be hard if (Λ, x_0) and (Λ, x_1) are indistinguishable for a random $x_0 \in L$ and a random $x_1 \in X \backslash L$.

5 Construction of a Strongly Universal$_2$ Projective Hash-Family

One constructs this family using the algebraic techniques given in [8]. The steps are as follows.

1. First construct a subset-membership problem.
2. Then construct a diverse group system.
3. From this construct a strongly universal$_1$ projective hash family.
4. Finally from this construct, using a collision-resistant hash funtion(CRHF), a strongly universal$_2$ projective hash family.

5.1 The Subset-Membership Problem

Let G be a bilinear group and $e : G \times G \to \tilde{G}$ be a bilinear map, where G and $\tilde{G}$ are groups of prime order q. We use additive notation for G and multiplicative notation for $\tilde{G}$. With $G, \tilde{G}, q$ and e given, we now define an instance of a subset-membership problem as follows.

Let g_0, g_1, g_2 be randomly chosen elements of G. Define $X = G \times \tilde{G}$ and let L be the subgroup of X generated by $(g_0, e(g_1, g_2))$. A witness for $(x_0, x_1) \in L$ is a $w \in Z_q$ such that $(x_0, x_1) = (wg_0, e(g_1, g_2)^w)$. Obviously, one can efficiently sample a random element of L, together with a witness by generating $w \in Z_q$ at random and computing $(wg_0, e(g_1, g_2)^w)$.

It is clear that this defines a subset-membership problem (distinguishing between elements of L and $X \backslash L$) and we will show that the hardness of this subset-membership problem reduces to the DBDH-assumption as follows.

We have to show that it is hard to distinguish tuples of the form

$$(g_0, g_1, g_2, rg_0, A = e(g_1, g_2)^r)$$

from the tuples of the form

$$\left(g_0, g_1, g_2, rg_0, B = e(g_1, g_2)^{r'}\right),$$

where g_0, g_1, g_2 are randomly chosen from G and r, r' are randomly chosen from Z_q.

Now we show how to derive an instance for DBDH problem from the given tuples. We set

$$(g = g_0, A = ag = rg_0, B = bg = g_1, C = cg = g_2, Z = A)$$

and

$$(g = g_0, A = ag = rg_0, B = bg = g_1, C = cg = g_2, Z = B)$$

It is clear, that for $Z{=}A$ the distribution of the corresponding tuple is from $\mathbf{D}$, as $Z = A = e(g_1, g_2)^r = e(bg, cg)^a = e(g, g)^{abc}$. If $Z{=}B$, then clearly the distribution of the corresponding tuple is from $\mathbf{R}$. This shows that if we can solve DBDH problem then we can solve the above subset-membership problem.

5.2 Construction of Diverse Group-System

Now as we have the subset-membership problem, we can construct a Diverse Group System as follows.

We set, for fixed non-zero element $g_0 \in G$, $f(x) = e(g_0, x)$ for all $x \in G$. This is clearly an isomorphism. With X and L defined as above, set

$K = Z_q \times Z_q$. We define for each $(k_0, k_1) \in K$

a map $H_{k_0,k_1} : G \times \tilde{G} \to \tilde{G}$ as follows.

For $(x, y) \in X = G \times \tilde{G}$, $H_{k_0,k_1}(x, y) = f(x)^{k_0} y^{k_1}$.

It can be cheked that the correspondence $(k_0, k_1) \rightarrow H_{k_0,k_1}$ is a bijection between K and $\mathrm{Hom}(X, \tilde{G})$,the set of all group homomorphisms from X to $\tilde{G}$ (Its clear that $\mathrm{Hom}(X, \tilde{G})$ is a group).

With H=Hom$(X, \tilde{G})$, we consider the group system $\mathbf{G}$= $(H, X, L, \tilde{G})$.

Claim : $\mathbf{G}$ is a diverse group system.

Given $\mathbf{G}$= $(H, X, L, \tilde{G})$ with $g_0, g_1, g_2 \in G$ with $X = G \times \tilde{G}$ and $L =< (g_0, e(g_1, g_2)) >$ a subgroup of X generated by $(g_0, e(g_1, g_2))$, we set $X' = \tilde{G} \times \tilde{G}$ and $L' =< (f(g_0), e(g_1, g_2)) >$ a subgroup of X' generated by $(f(g_0), e(g_1, g_2))$.

With H=Hom$(X, \tilde{G})$ we consider H'=Hom$(X', \tilde{G})$. In [8] one can see that, the map $(k_0, k_1) \rightarrow H'_{(k_0,k_1)}$, where $H'_{k_0,k_1}(x, y) = x^{k_0} y^{k_1}$ is a 1-1 correspondence between $K = Z_q \times Z_q$ and H'=Hom$(X', \tilde{G})$. So now we have the following two group systems.

$\mathbf{G}$=$(H, X, L, \tilde{G})$ and $\mathbf{G}'$=$(H', X', L', \tilde{G})$.

We know (by [8]) that $\mathbf{G}'$=$(H', X', L', \tilde{G})$ is a diverse group system .

We will show that $\mathbf{G}$=$(H, X, L, \tilde{G})$ is a diverse group system.

The map $(k_0, k_1) \rightarrow H_{(k_0,k_1)}$, where $H_{k_0,k_1}(x, y) = f(x)^{k_0} y^{k_1}$

is a 1-1 correspondence between $Z_q \times Z_q$ and H

Now let (x', y') be an element which is in $X \backslash L$. Then $(x', y') = (ag_0, e(g_1, g_2)^b)$ for some $a \neq b$, $a, b \in Z_q$. We have to show that there exists $(k_0, k_1) \in Z_q \times Z_q$ such that $H_{(k_0,k_1)}(x', y') = f(x')^{k_0}.y'^{k_1} \neq 0$ but $H_{(k_0,k_1)}$ vanishes on L. Now $(f(x'), y') = (f(g_0)^a, e(g_1, g_2)^b)$, clearly $(f(x'), y') \in X' \backslash L'$. As $\mathbf{G}'$ is a diverse group system there exists a tuple $(k_0, k_1) \in Z_q \times Z_q$ such that the corresponding homomorphism H'_{k_0,k_1} vanishes on L' but $H'_{k_0,k_1}(f(x'), y') = f(x')^{k_0} y'^{k_1} \neq 0$. Since $H'_{k_0,k_1}(f(x), y) = H_{k_0,k_1}(x, y)$ for all $(x, y) \in X$, $H_{(k_0,k_1)}$ vanishes on L and $H_{(k_0,k_1)}(x', y') \neq 0$.

This clearly shows that $\mathbf{G}$=$(H, X, L, \tilde{G})$ is a diverse group system.

5.3 Construction of Strongly Universal$_2$ Projective Hash Family

Now we construct a universal$_1$ projective hash family $\mathbf{H}$ =$(H, K, X, L, \Pi, S, \alpha)$ from the above group system using the technique in [8].

With H, K, X, L as above we set $\Pi = \tilde{G}$ and $S = \tilde{G}$. The map $\alpha : K \rightarrow S$ is defined as follows :

α maps $(k_0, k_1) \in K$ to $H_{k_0,k_1}(g_0, e(g_1, g_2)) = f(g_0)^{k_0} e(g_1, g_2)^{k_1} \in \tilde{G}$. By [8] the resulting family is clearly universal$_1$ projective hash family. We now construct strongly universal$_2$ projective hash family using this family.

Let $\Gamma : X \times \tilde{G} \rightarrow Z_q$ be a collision resistant hash function (CRHF).

Now we define $\hat{\mathbf{H}}$=$(\hat{H}, K \times K, X \times \tilde{G}, L \times \tilde{G}, \tilde{G}, S \times S, \hat{\alpha})$. For $((k_0, k_1), (k'_0, k'_1)) \in K \times K$, $(x, y) \in X$ and $e \in \tilde{G}$, define

$$\hat{H}_{((k_0,k_1),(k'_0,k'_1))}((x, y), e) = H_{(k_0,k_1)}(x, y).(H_{(k'_0,k'_1)}(x, y))^t$$

where $\Gamma((x, y), e) = t$. Then define $\hat{\alpha}((k_0, k_1), (k'_0, k'_1)) = (\alpha(k_0, k_1), \alpha((k'_0, k'_1))$. Going by the arguments of [8], the above defined family is strongly universal$_2$ hash family.

Now once we obtain the strongly universal$_2$ projective hash family, using the Kurosawa and Desmedt [3] paradigm for hybrid public key encryption we can obtain an adaptively chosen ciphertext secure hybrid public-key encryption scheme whose seurity is based on the Decisional Bilinear Diffie-Hellman Problem.

For completeness we give Kurosawa-Desmedt's [3] generic construction for Hybrid-Encryption Scheme based on Hash Proof Systems:

Let SMP be a subset membership problem. A hash proof system (HPS) P for SMP associates with each instance $\Lambda[X, L, W, R]$ of SMP a projective hash family $(H, K, X, L, \Pi, S, \alpha)$.

5.4 Hybrid Scheme

Let SMP be a subset membership problem and P be a hash proof system for SMP. Let SKE be a one-time symmetric-key encryption [3] scheme.

Key Generation: Generate an instance $\Lambda[X, L, W, R]$ using the instance sampling algorithm of SMP. Suppose that P associates with $\Lambda[X, L, W, R]$ a projective hash family $(H, K, X, L, \Pi, S, \alpha)$. Choose $k \in K$ at random and compute $s = \alpha(k)$.
The public key is 's' and the secret key is 'k'. Let $T : \Pi \rightarrow \{0,1\}^l$ be a hash function, where l is the key-length for SKE. Its require that $T(u)$ is uniformly distributed over $\{0,1\}^l$ if u is uniformly distributed over Π.

Encryption: To encrypt a message m, generate $x \in L$ at random together with a witness $w \in W$ for x using the subset sampling algorithm of SMP. Compute $\pi = H_k(x)$ using the input s, x and w (by projectiveness of the hash family). Compute $\tilde{K} = T(\pi)$ and C=SKE.Enc$(\tilde{K}, m)$. The ciphertext is (x, C)

Decryption: To decrypt a ciphertext (x, C), compute $\pi = H_k(x)$ using the secret key k and x. Then decrypt C under $\tilde{K}$ using SKE.Dec and compute the resulting decryption m. (m may be reject.)

Theorem 1 (Kurosawa-Desmedt [3]). *The Hybrid encryption scheme is IND-CCA2 secure provided SMP is hard and the associated projective hash family is strongly universal$_2$ for each instance $\Lambda[X, L, W, R]$ and the symmetric-key encryption scheme SKE is secure in the sense of IND-CCA2 [3] and it is ϵ-rejection [3] secure for negligible ϵ .*

Now using our strongly universal$_2$ projective hash family and applying the Kurosawa-Desmedt paradigm, we can obtain an IND-CCA2 secure hybrid public-key encryption. Clearly the security of the scheme is based on the Decisional Bilinear Diffie-Hellman problem.

6 A Public-Key Encryption Based on PDDH

Let G be a bilinear group and $e : G \times G \rightarrow \tilde{G}$ be a bilinear map, where G and $\tilde{G}$ are groups of prime order q. We use multiplicative notation for group operation in G and $\tilde{G}$. We require a hash function $h : \tilde{G} \times G \times G \rightarrow Z_q$ with the following property, if a element is uniformly distributed in $\tilde{G} \times G \times G$ then its image under h be also uniformly distributed in Z_q.

Key Generation. A user's public/private key pair generation algorithm proceeds as follows. First choose elements $g, g_2 \in G$ at random. Then choose $\alpha \in_R Z_q$. Also choose elements $x^{'}, x_1, ..., x_n \in_R Z_q^*$ and $y^{'}, y^1, ..., y_n \in_R Z_q^*$. Next compute $g_1 = g^{\alpha}$, $e(g_1, g_2)$

$$u^{'} = g_2^{x^{'}} g^{y^{'}} \text{ and for } i = 1 \text{ to } n, u_i = g_2^{x_i} g^{y_i}$$

where n is a large positive integer. Now choose $id = (d_1, ..., d_n) \in_R \{0,1\}^n$. Compute $T = (u^{'} \prod_{i=1}^{n} u_i^{d_i})$, $l_1 = x^{'} + \sum_{i=1}^{n} d_i x_i$ and $l_2 = y^{'} + \sum_{i=1}^{n} d_i y_i$.
The public-key is $(g, g_2, e(g_1, g_2), T, h)$ and the secret-key is (g_1, l_1, l_2).

Encryption. For a message $m \in \tilde{G}$, the encryption algorithm under the public-key runs as follows.
1. Choose $t \in_R Z_q^*$,
2. Compute $c_1 = g_2^t$, $c_2 = g^t$ and $e(g_1, g_2)^t$,
3. Compute $T^t = (u^{'} \prod_{i=1}^{n} u_i^{d_i})^t$,

4. $\pi = (e(g_1, g_2)^t, c_2, T^t)$ 5. Compute $r = h(\pi)$,
6. Compute $c_3 = e(g_1, g_2)^{rt}.m$.
The ciphertext is (c_1, c_2, c_3).

Decryption. Given a ciphertext (c_1, c_2, c_3) encrypted with the above public-key, the decryption algorithm runs as follows. For the secret key (g_1, l_1, l_2),
compute $e(g_1, c_1)$, compute $c_1^{l_1}.c_2^{l_2}$,
compute $r = h(e(g_1, c_1), c_2, c_1^{l_1}.c_2^{l_2})$,
compute $m = c_3.(e(g_1, c_1)^r)^{-1}$.

We first verify that this is an encryption scheme, in the sense that the decryption of an encryption of a message yields the message. Since $c_1 = g_2^t$, $c_2 = g^t$, this implies

$$\begin{aligned} c_1^{l_1}.c_2^{l_2} &= (g_2^t)^{x' + \sum_{i=1}^n d_i x_i}.(g^t)^{y' + \sum_{i=1}^n d_i y_i} \\ &= (g_2^{x' + \sum_{i=1}^n d_i x_i}.g^{y' + \sum_{i=1}^n d_i y_i})^t \\ &= ((g_2^{x'}.g^{y'})(g_2^{\sum_{i=1}^n d_i x_i}.g^{\sum_{i=1}^n d_i y_i}))^t \\ &= (u' \prod_{i=1}^n u_i^{d_i})^t \\ &= T^t \end{aligned}$$

and also $e(g_1, c_1)$=$e(g_1, g_2^t)$=$e(g_1, g_2)^t$.
So $r = h(e(g_1, c_1), c_2, c_1^{l_1}.c_2^{l_2})$=$h(e(g_1, g_2)^t, c_2, T^t) = h(\pi)$.
Hence $c_3.(e(g_1, c_1)^r)^{-1}$=$e(g_1, g_2)^{rt}.m.(e(g_1, g_2^t)^r)^{-1} = e(g_1, g_2)^{rt}.m.(e(g_1, g_2)^{rt})^{-1} = m$.

Note: Keeping $id = (d_1, ..., d_n)$, $x', x_1, ..., x_n \in_R Z_q^*$ and $y', y^1, ..., y_n \in_R Z_q^*$ as a part of secret key will give the key l_1, l_2.

6.1 security

Theorem 2. *The scheme A is secure against indistinguishability attack provided Pairing Decision Diffie-Hellman(PDDH) is hard for the pairing friendly groups G, $\tilde{G}$ and the hash function h satisfies the requisite property as mentioned in the scheme A.*

Proof. Assuming there exists a Adversary who have non-negligible advantage in the indistinguishability attack against the scheme A we build a simulator who in turn use the above adversary to solve the PDDH problem. Let the simulator is given an instance $\{\tilde{g}, g, g_2, \tilde{g}^{r_1}, g^{r_2}, g_2^{r_2}\}$ of the PDDH problem. Without any loss of generality one can assume $\tilde{g}$ to be of the form $e(g_1, g_2)$ for some unknown $g_1 \in G$. So now the instance becomes

$$\{g, g_2, e(g_1, g_2), e(g_1, g_2)^{r_1}, g^{r_2}, g_2^{r_2}\}.$$

. One should know that given $e(g_1, g_2)$ and g_2, its hard to compute g_1. We now give the details of the simulator. First it chooses an $id = (d_1, ..., d_n) \in_R \{0, 1\}^n$. Then it chooses $x', x_1, ..., x_n \in_R Z_q^*$ and $y', y_1, ..., y_n \in_R Z_q^*$. Now it computes $l_1 = x' + \sum_{i=1}^n d_i x_i$, $l_2 = y' + \sum_{i=1}^n d_i y_i$, $u' = g_2^{x'} g^{y'}$ and for $i = 1$ to $n, u_i = g_2^{x_i} g^{y_i}$. and $T = (u' \prod_{i=1}^n u_i^{d_i})$. Now the simulator gives the following tuple $(g, g_2, e(g_1, g_2), T, h)$ as public key to the adversary where h is the hash function required for the scheme.

Now the adversary issues two messages m_0, m_1. To this simulator chooses $b \in_R \{0,1\}$ and encrypt m_b as follows. It computes
$\pi = (e(g_1,g_2)^{r_1}, g^{r_2}, (g_2^{r_2})^{l_1}.(g^{r_2})^{l_2})$,
$r = h(\pi)$ and $C = e(g_1,g_2)^{r.r_1}.m_b$ and output $(g^{r_2}, g_2^{r_2}, C)$.

This completes the description of the simulator. Now we show that if the input comes from **D** then the simulation is perfect and hence the adversary will have non-negligible advantage in guessing the hidden bit. We will also show that if the input comes from **R**, then the adversary's view is essentially independent of the hidden bit b, i.e. $Pr(b = \hat{b})$ is close to $\frac{1}{2}$, and therefore the adversary's advantage is negligible. Running the simulator and adversary together, we have a distinsuishing algorithm for **R** and **D** as follows. If the bit b and the adversary's output bit $\hat{b}$ matches then simulator outputs 1, otherwise it outputs 0. In view of the above, this will give a distinguishing algorithm.

Now we first show that when the input is from **D** the encryption of the message by the simulator if perfectly legitimate. As the input $\{g, g_2, e(g_1,g_2), e(g_1,g_2)^{r_1}, g^{r_2}, g_2^{r_2}\}$ is from **D**, this implies that $r_1 = r_2 = t$ (say). Now Going by the description of the encryption oracle of the simulator we have,

$$\begin{aligned}
\pi &= (e(g_1,g_2)^t, g^t, (g_2^t)^{l_1}.(g^t)^{l_2}) \\
&= (e(g_1,g_2)^t, g^t, (g_2^t)^{x' + \sum_{i=1}^n d_i x_i}.(g^t)^{y' + \sum_{i=1}^n d_i y_i}) \\
&= (e(g_1,g_2)^t, g^t, (g_2^{x' + \sum_{i=1}^n d_i x_i}.g^{y' + \sum_{i=1}^n d_i y_i})^t) \\
&= (e(g_1,g_2)^t, g^t, ((g_2^{x'}.g^{y'})(g_2^{\sum_{i=1}^n d_i x_i}.g^{\sum_{i=1}^n d_i y_i}))^t) \\
&= (e(g_1,g_2)^t, g^t, (u' \prod_{i=1}^n u_i^{d_i})^t) \\
&= (e(g_1,g_2)^t, g^t, T^t)
\end{aligned}$$

$r = h(\pi)$ and $C = e(g_1,g_2)^{rt}.m_b$ which clearly shows that simulator outputs a perfectly legitimate ciphertext of the message m_b.

Now we show that when the input is from **R**, the output of the encryption oracle is not a legitimate ciphertext but 'random'. As the input $\{g, g_2, e(g_1,g_2), e(g_1,g_2)^{r_1}, g^{r_2}, g_2^{r_2}\}$ is from **R** this implies $r_1 \neq r_2$ and this makes π a random element in $(\tilde{G} \times G \times G)$ and hence by the property of the hash function $h(\pi)$ become a random element which in turn makes $C = e(g_1,g_2)^{r_1.r}.m_b$ a uniformly distributed element and hence random to adversary's view. □

7 Conclusions

We presented a hybrid public-key encryption scheme, which is secure against adaptive chosen ciphertext attack, using Kurosawa-Desmedt paradigm. The security of the scheme is based on the Decisional Bilinear Diffie-Hellman problem. We also introduce a new intractibility assumption for pairing friendly groups. We propose a public-key encryption scheme and proved its security against indistinguishability attack based on the hardness of the new assumption.

References

1. A. Joux and K. Nguyen. Separating Decision Diffie-Hellman from Diffie-Hellman in cryptographic groups. Available at eprint.iacr.org.
2. D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. In STOC. ACM Press, 1991.

3. K. Kurosawa and Y. Desmedt. A new paradigm of hybrid encryption scheme. In M. Franklin editor, Advances in Cryptology- Crypto 2004, volume 3152 of Lecture Notes in Computer Science, pages 426-442. Springer-Verlag, 2004.
4. M. Bellare and P. Rogaway. Optimal Asymmetric Encryption - How to encrypt with RSA. In EUROCRYPT '94, volume 839 of LNCS, pages 93-111. Springer-Verlag, 1994.
5. M. Bellare and P. Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In First ACM *Conference on Computer and Communications Security*, pages 62-73, 1993.
6. M. Naor and M. Yung. Public-Key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks. In 22nd Annual ACM Symposium on Theory of Computing, pages 427-437, 1990.
7. R. Cramer and V. Shoup. A Practical Publlic-Key Cryptosystem Provably Secure Against Addaptive Chosen Cip hertext Attacks. In Proc. CRYPTO '98, Springer Verlag LNCS, 1998.
8. R. Cramer and V. Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. Cryptology ePrint Archive. Available at `http://eprint.iacr.org/2001/085.pdf`.
9. V. Shoup. Lower bounds for discrete logarithms and related problems. In *Advances in Cryptology-Eurocrypt* '98,1998.