# A Generic Hybrid Encryption Construction in the Quantum Random Oracle Model

Presented by: Angela Robinson

Department of Mathematical Sciences, Florida Atlantic University

April 4, 2018

Shor's Algorithm (1994) solves the following problems in quantum polynomial-time

- the integer factorization problem
- the discrete logarithm problem
- elliptic-curve discrete logarithm problem

Progress in the area of quantum information and computation has influenced the growth of *quantum-resistant* cryptography.

- Defeated cryptosystems: RSA, DSA, Elliptic Curve-based, ...
- Potential survivors: Code-, lattice-, multivariate-, isogeny-, and hash-based

Symmetric key encryption

- Usually faster runnning times
- Requires a shared secret in advance of the protocol

Asymmetric encryption

- Does not require a shared secret between sender and recipient
- Can run slower for long messages

### Hybrid Encryption idea

Encrypt message using symmetric component under random string $k$, then encrypt $k$ under the asymmetric component

## IND-CCA

An encryption scheme satisfies *indistinguishability under chosen-ciphertext attack* if, given access to the decryption oracle, the advantage of an adversary $\mathcal{A}$ winning this game is negligible:

- $\mathcal{A}$ selects two messages $m_0, m_1$ and sends to a challenger $\mathcal{C}$
- $\mathcal{C}$ selects $b \in_R \{0, 1\}$ and sends $c_b = \mathrm{Enc}(m_b)$ to $\mathcal{A}$
- $\mathcal{A}$ submits $b^* \in \{0, 1\}$ to $\mathcal{C}$ and wins if $b = b^*$.

## Naive approach

Combine IND-CCA secure symmetric component with IND-CCA secure asymmetric component to achieve IND-CCA secure hybrid encryption.

# Fujisaki Okamoto transform

## Weaker security assumptions

Fujisaki and Okamoto (1999) combined one-time symmetric encryption with one-way asymmetric encryption to achieve IND-CCA security.

$$\mathsf{HY.Enc}_{pk}(m) = \mathsf{ASYM.Enc}_{pk}(r; H(r,m)) || \mathsf{SYM.Enc}_{G(r)}(m)$$

Observations:

- The *asymmetric* component encrypts randomness $r$
- The *symmetric* component encrypts message $m$ under hash of randomness $r$
- There are, in a sense, two components.

# Unruh's QROM-secure Fujisaki Okamoto

## Security in QROM

Targhi and Unruh show how to modify FO transform to achieve security in the QROM.

$\mathrm{HY.Enc}_{pk}(m; r) =$
$\mathrm{ASYM.Enc}_{pk}(r; H(r||\mathrm{SYM.Enc}_{G(r)}(m))), \mathrm{SYM.Enc}_{G(r)}(m), H^{'}(r)$
Observations:

- The *asymmetric* component encrypts randomness $r$
- The *symmetric* component encrypts message $m$ under hash of randomness $r$
- There is a third component that is simply the hash value of randomness $r$

## Our contribution: QROM-secure Hybrid Encryption

Let $\mathsf{KEM.Enc}(1^n, pk; r) = (k, c)$.
Our QROM-secure hybrid construction is:

$$\mathsf{HY.Enc}_{pk}(m; r) = c, \mathsf{SYM.Enc}_{G(k)}(m), H(k||r).$$

Observations:

- The *asymmetric* component is the ciphertext of an encapsulated key $k$
- The *symmetric* component encrypts message $m$ under hash of encapsulated key $k$
- The third component is the hash value of encapsulated key $k$ with random string $r$.

## One-way secure

An asymmetric encryption scheme is said to be *one-way* if no polynomial-time adversary $\mathcal{A}$ can recover the whole plaintext from a given ciphertext.

## One-time secure

A symmetric encryption scheme is *one-time secure* if no polynomial-time adversary $\mathcal{A}$ can distinguish between the encryption of two messages when a fresh key is used for encryption.

## Classical Random Oracle

- Theoretical black box
- Responds to every unique query with a *truly* random response
- Disadvantage: cannot be implemented in polynomial space
- Advantage: enables security proofs, can be *simulated* in polynomial time and space

A cryptosystem in the **random oracle model** is a cryptosystem where one or more hash functions are replaced by oracle queries to the random function.

## Quantum information

- Described by *qubits*
- A single qubit can have a state of $|0\rangle$, $|1\rangle$, or any linear combination
$$\alpha_0 |0\rangle + \alpha_1 |1\rangle$$
satisfying $\alpha_0, \alpha_1 \in \mathbb{C}$ where $|\alpha_0|^2 + |\alpha_1|^2 = 1$
- Observation permanently alters the state of a qubit

## Differences between QRO and RO

- There is no "transcript" of all queries to QRO
- Queries to the QRO in a "superposition" of all possible hash function inputs are allowed.

## KEM

Let $\Pi^{\text{KEM}} = (\text{KEM.Gen}, \text{KEM.Enc}, \text{KEM.Dec})$ be a key encapsulation mechanism with

- coinspace $\text{COIN}^{\text{KEM}} = \{0,1\}^{n_1}$
- key space $\mathcal{K}^{\text{KEM}} = \{0,1\}^{n_2}$
- ciphertext space $\mathcal{C}^{\text{KEM}} = \{0,1\}^{n_3}$.

The parameters $n_1, n_2, n_3$ depend on the security parameter $n$ and should each be of size $2^{\omega(\log n)}$.

# Generic Hybrid Encryption Scheme



$\Pi^{\mathsf{KEM}}$ consists of the following three algorithms:

$$\mathsf{KEM.Gen}(1^n) \rightarrow (pk, sk)$$
$$\mathsf{KEM.Enc}(1^n, pk; r) \rightarrow (k, c)$$
$$\mathsf{KEM.Dec}(c, sk) \rightarrow (k, r) \text{ or } \perp .$$

## $\delta$-spread

A key encapsulation mechanism is $\delta$-spread if for every *pk* generated,

$$max_{y \in \{0,1\}^*} \Pr[y = c | (k, c) \leftarrow \mathsf{KEM.Enc}(1^n, pk; r), r \xleftarrow{\$} \mathsf{COIN}^{\mathsf{KEM}}] \leq \frac{1}{2^{-\delta}}.$$

As defined, by Unruh, we say that the KEM $\Pi^{\mathsf{KEM}}$ is well-spread if $\delta = \omega(\log(n))$.

Let $\Pi^{\mathsf{SYM}} = (\mathsf{SYM.Enc}, \mathsf{SYM.Dec})$ be a symmetric encryption scheme with key space $\mathcal{K}^{\mathsf{SYM}}$, and message space $\mathcal{M}^{\mathsf{SYM}}$.

## Two hash functions

$$H : \{0,1\}^{n_2} \to \mathcal{K}^{\mathsf{SYM}}$$
$$G : \{0,1\}^{n_1+n_3} \to \{0,1\}^{l}$$

The hybrid encryption scheme Enc, on input $m$ and security parameter $n$ runs as follows:

1. Gen runs $\text{KEM.Gen}(1^n)$ to produce $(pk, sk)$
2. Enc chooses $r \xleftarrow{\$} \text{COIN}^{\text{KEM}}$, then runs $\text{KEM.Enc}(1^n, pk; r) = (k, c)$. Enc defines
   - $\alpha := c$
   - $\beta := \text{SYM.Enc}_{G(k)}(m)$
   - $\gamma := H(k||r)$
3. Enc returns ciphertext $(\alpha, \beta, \gamma)$

# Generic Hybrid Encryption Scheme

The hybrid decryption scheme Dec, on input $(\alpha, \beta, \gamma), sk$ runs as follows:

1. Compute $(k, r) :=$ KEM.Dec$(\alpha, sk)$. If value is $\perp$, return $\perp$.
2. If $\gamma \neq H(k||r)$, return $\perp$.
3. Otherwise, $m :=$ SYM.Dec$_{G(k)}(\beta)$. Return $m$.

**Theorem**

*The hybrid scheme $\Pi^{\mathsf{HY}}$ is IND-CCA secure in the quantum random oracle model if $\Pi^{\mathsf{KEM}}$ is one-way secure and well-spread, and if $\Pi^{\mathsf{SYM}}$ is one-time secure.*

# Security Proof - Game 0

Generate:

$$H \xleftarrow{\$} \Omega_H,\ G \xleftarrow{\$} \Omega_G$$

$$(pk, sk) \xleftarrow{\$} \mathsf{KEM.Gen}(1^n),\ r \xleftarrow{\$} \mathsf{COIN}^{\mathsf{KEM}}$$

$$m_0, m_1 \leftarrow \mathcal{A}_{hy}^{G,H,\mathsf{Dec}}(pk)$$

$$b \xleftarrow{\$} \{0,1\}$$

Challenge:

$$(k^*, c^*) \xleftarrow{\$} \mathsf{KEM.Enc}(1^n, pk; r)$$

$$\alpha^* \leftarrow c^*$$

$$\beta^* \leftarrow \mathsf{SYM.Enc}_{G(k^*)}(m_b)$$

$$\gamma^* \leftarrow H(k^* || r)$$

Guess:

$$b' \leftarrow \mathcal{A}_{hy}^{G,H,\mathsf{Dec}}(\alpha^*, \beta^*, \gamma^*)$$

Return $b = b'$

We must apply OW2H Lemma by Unruh.

### Lemma

*One Way to Hiding Lemma: Let* $H : \{0,1\}^{l_1} \to \{0,1\}^{l_2}$ *be a random oracle. Consider an oracle algorithm* $\mathcal{A}_1$ *that makes at most* $q$ *queries to* $H$*. Let* $\mathcal{C}_1$ *be an oracle algorithm that on input* $x$ *does the following:*

1. *Pick* $i \xleftarrow{\$} \{1, \ldots, q\}, y \xleftarrow{\$} \{0,1\}^{l_2}$
2. *Run* $\mathcal{A}_1^H(x, y)$ *until (just before) the* $i$*-th query.*
3. *Measure the argument of the query in the computational basis and return the measurement outcome. If* $\mathcal{A}_1^H$ *makes less than* $i$ *queries to* $H$*, then return* $\perp$*.*

Let $P^1_{\mathcal{A}}, P^2_{\mathcal{A}}, P_{\mathcal{C}}$ be defined as follows:

$$P^1_{\mathcal{A}} := \Pr[b' = 1 | H \xleftarrow{\$} \Omega_H, x \xleftarrow{\$} \{0,1\}^{l_1}, b' \leftarrow \mathcal{A}^H_1(x, H(x))]$$

$$P^2_{\mathcal{A}} := \Pr[b' = 1 | H \xleftarrow{\$} \Omega_H, x \xleftarrow{\$} \{0,1\}^{l_1}, b' \leftarrow \mathcal{A}^H_1(x, y)]$$

$$P_{\mathcal{C}} := \Pr[x' = x | H \xleftarrow{\$} \Omega_H, x \xleftarrow{\$} \{0,1\}^{l_1}, x' \leftarrow \mathcal{C}^H_1(x, i)]$$

Then

$$|P^1_{\mathcal{A}} - P^2_{\mathcal{A}}| \leq 2q\sqrt{P_{\mathcal{C}}}.$$

Proof by sequence of security games. Combining probabilities, this yields an upper bound on the success probability in Game 0:

$$\Pr[1 \leftarrow \mathit{Game}0] < \frac{1}{2} + \mathit{negl}(n)^{\mathrm{KEM}} + \mathit{negl}(n)^{\mathrm{SYM}} + 2q\sqrt{2^{-\omega(\log n)}}.$$

This scheme contributes IND-CCA secure hybrid encryption scheme believed to be quantum-resistant.

# Potential constructions

- BIKE-KEM + AES-GCM
- Frodo-KEM + AES-GCM
- Kyber-KEM + AES-GCM

https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

# References


- “Secure Integration of Asymmetric and Symmetric Encryption Schemes”, Fujisaki, Eiichiro and Okamoto, Tatsuaki, CRYPTO ’99, 1999
- “Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms”, Targhi, Ehsan Ebrahimi and Unruh, Dominique, 14th International Conference on Theory of Cryptography, 2016
- “REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform”, Okamoto, Tatsuaki and Pointcheval, David, Proceedings of the 2001 Conference on Topics in Cryptology, 2001
- *Quantum Computation and Quantum Information* by Nielsen and Chuang, 2000

Additional slides

## Formal Security Definitions

### One-way secure

**Definition**

A key encapsulation mechanism $\Pi^{\mathsf{KEM}} = (\mathsf{KEM.Gen}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$ is *one-way secure* if no quantum polynomial-time adversary $\mathcal{A}$ can win in the $Game^{\mathsf{OW}}_{\mathcal{A},\Pi^{\mathsf{KEM}}}(n)$ game, except with probability at most $negl(n)^{\mathsf{KEM}}$:

KeyGen: The challenger $\mathcal{C}$ runs $\mathsf{KEM.Gen}(1^n)$ to obtain a pair of keys $(pk, sk)$

Query: $\mathcal{C}$ selects $r \xleftarrow{\$} \mathsf{COIN}^{\mathsf{KEM}}$ and runs $\mathsf{KEM.Enc}(1^n, pk; r)$ to obtain a random key and ciphertext pair $(k, c)$. $\mathcal{C}$ sends $c$ to $\mathcal{A}$.

Guess: The adversary on input $(pk, c)$ produces a bit string $k'$ and wins if $k = k'$.

## Definition

A symmetric encryption scheme $\Pi^{\mathsf{SYM}} = (\mathsf{SYM.Enc}, \mathsf{SYM.Dec})$ is *one-time secure* if no quantum polynomial-time adversary $\mathcal{A}$ can win in game $Game^{\mathsf{OT}}_{\mathcal{A},\Pi^{\mathsf{SYM}}}(n)$, except with probability at most $\frac{1}{2} + negl(n)^{\mathsf{SYM}}$:

KeyGen: The challenger $\mathcal{C}$ picks a key $k \xleftarrow{\$} \mathcal{K}^{\mathsf{SYM}}$

Query: On input $1^n$, $\mathcal{A}$ chooses two messages $m_0, m_1$ of the same length and sends them to the challenger. $\mathcal{C}$ chooses $b \xleftarrow{\$} \{0,1\}$ and responds with $c \xleftarrow{\$} \mathsf{SYM.Enc}_k(m_b)$

Guess: $\mathcal{A}$ produces a bit $b'$ and wins if $b = b'$.

## Definition

A hybrid encryption scheme $\Pi^{HY}$ is IND-CCA in the QROM if no efficient quantum adversary $\mathcal{A}$ can win in the $Game^{\mathsf{CCA-QRO}}_{\mathcal{A},\Pi^{\mathsf{HY}}}(n)$, except with probability at most $\frac{1}{2} + negl(n)$:

KeyGen: The challenger runs Gen on input $n$, which runs KEM.Gen$(1^n)$ to produce $(pk, sk)$.

Query: The adversary $\mathcal{A}$ is given the public key $pk$ along with classical access to the decryption oracle and quantum access to the random oracles $G, H$. $\mathcal{A}$ chooses two messages $m_0, m_1$ of the same length and sends them to the challenger $\mathcal{C}$. $\mathcal{C}$ chooses $b \xleftarrow{\$} \{0, 1\}$ and responds with $c \leftarrow Enc_{pk}(m_b)$.

Guess: $\mathcal{A}$ continues to send classical decryption queries to Dec, but may not query $c$. $\mathcal{A}$ also sends quantum queries to random oracles $G, H$.