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
Motivation
Hybrid Encryption

Symmetric key encryption
- Usually faster running 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
Hybrid Encryption
Security Definitions

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 $c_b = \text{Enc}(m_b)$ 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 Okamato transform

Weaker security assumptions

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

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

Observations:

- The \textit{asymmetric} component encrypts randomness \( r \)
- The \textit{symmetric} component encrypts message \( m \) under hash of randomness \( r \)
- There are, in a sense, two components.
Security in QROM

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

\[
\text{HY.Enc}_{pk}(m; r) = \\
\text{ASYM.Enc}_{pk}(r; H(r || \text{SYM.Enc}_{G(r)}(m))), \text{SYM.Enc}_{G(r)}(m), H'(r)
\]

Observations:

- The \textit{asymmetric} component encrypts randomness \( r \)
- The \textit{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 $\text{KEM.Enc}(1^n, pk; r) = (k, c)$.
Our QROM-secure hybrid construction is:

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

Observations:

- The \emph{asymmetric} component is the ciphertext of an encapsulated key $k$
- The \emph{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 $r$. 
Hybrid Encryption
Security Definitions

**One-way secure**
An asymmetric encryption scheme is said to be *one-way* if no polynomial-time adversary $A$ 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 $A$ 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

\( \Pi^{\text{KEM}} \) consists of the following three algorithms:

\[
\begin{align*}
\text{KEM.Gen}(1^n) & \rightarrow (pk, sk) \\
\text{KEM.Enc}(1^n, pk; r) & \rightarrow (k, c) \\
\text{KEM.Dec}(c, sk) & \rightarrow (k, r) \text{ or } \perp .
\end{align*}
\]

**\( \delta \)-spread**

A key encapsulation mechanism is \( \delta \)-spread if for every \( pk \) generated,

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

As defined, by Unruh, we say that the KEM \( \Pi^{\text{KEM}} \) is well-spread if \( \delta = \omega(\log(n)) \).
Let $\Pi^{\text{SYM}} = (\text{SYM.Enc}, \text{SYM.Dec})$ be a symmetric encryption scheme with key space $\mathcal{K}^{\text{SYM}}$, and message space $\mathcal{M}^{\text{SYM}}$.

Two hash functions

\[
H : \{0, 1\}^{n_2} \rightarrow \mathcal{K}^{\text{SYM}}
\]
\[
G : \{0, 1\}^{n_1 + n_3} \rightarrow \{0, 1\}^l
\]
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 $r \gets \text{COIN}^{\text{KEM}}$, 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 \((k, r) := \text{KEM}.\text{Dec}(\alpha, sk)\). If value is \(\perp\), return \(\perp\).
2. If \(\gamma \neq H(k \| r)\), return \(\perp\).
3. Otherwise, \(m := \text{SYM}.\text{Dec}_{G(k)}(\beta)\). Return \(m\).

**Theorem**

The hybrid scheme \(\Pi^{HY}\) is IND-CCA secure in the quantum random oracle model if \(\Pi^{KEM}\) is one-way secure and well-spread, and if \(\Pi^{SYM}\) is one-time secure.
Security Proof - Game 0

Generate:

\[
H \leftarrow \Omega_H,\ G \leftarrow \Omega_G
\]
\[
(pk,\ sk) \leftarrow \text{KEM.Gen}(1^n),\ r \leftarrow \text{COIN}^\text{KEM}
\]
\[
m_0,\ m_1 \leftarrow A^G,H,\text{Dec}(pk)
\]
\[
b \leftarrow \{0,\ 1\}
\]

Challenge:

\[
(k^*,\ c^*) \leftarrow \text{KEM.Enc}(1^n,\ pk;\ r)
\]
\[
\alpha^* \leftarrow c^*
\]
\[
\beta^* \leftarrow \text{SYM.Enc}_G(k^*)(m_b)
\]
\[
\gamma^* \leftarrow H(k^*\|r)
\]

Guess:

\[
b' \leftarrow A^G,H,\text{Dec}(\alpha^*,\ \beta^*,\ \gamma^*)
\]

Return \( b = b' \)
Generic Hybrid Encryption Scheme

Proof techniques

We must apply OW2H Lemma by Unruh.

Lemma
One Way to Hiding Lemma: Let $H : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$ be a random oracle. Consider an oracle algorithm $A_1$ that makes at most $q$ queries to $H$. Let $C_1$ be an oracle algorithm that on input $x$ does the following:

1. Pick $i \leftarrow \{1, \ldots, q\}$, $y \leftarrow \{0,1\}^{l_2}$
2. Run $A_1^H(x, y)$ until (just before) the $i$-th query.
3. Measure the argument of the query in the computational basis and return the measurement outcome. If $A_1^H$ makes less than $i$ queries to $H$, then return $\perp$. 
Let $P^1_A, P^2_A, P_C$ be defined as follows:

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

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

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

Then

$$|P^1_A - P^2_A| \leq 2q \sqrt{P_C}.$$
Proof by sequence of security games. Combining probabilities, this yields an upper bound on the success probability in Game 0:

$$\Pr[1 \leftarrow \text{Game0}] < \frac{1}{2} + \negl(n)^{\text{KEM}} + \negl(n)^{\text{SYM}} + 2q\sqrt{2^{-\omega(\log n)}}.$$ 

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

References

• “Secure Integration of Asymmetric and Symmetric Encryption Schemes”, Fujisaki, Eiichiro and Okamoto, Tatsuaki, CRYPTO ’99, 1999


• Quantum Computation and Quantum Information by Nielsen and Chuang, 2000
Additional slides
Formal Security Definitions

One-way secure

Definition

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

- **KeyGen**: The challenger $C$ runs KEM.Gen($1^n$) to obtain a pair of keys $(pk, sk)$
- **Query**: $C$ selects $r \leftarrow \text{COIN}^{\text{KEM}}$ and runs KEM.Enc($1^n, pk, r$) to obtain a random key and ciphertext pair $(k, c)$. $C$ sends $c$ to $A$.
- **Guess**: The adversary on input $(pk, c)$ produces a bit string $k'$ and wins if $k = k'$. 
Formal Security Definitions
One-time secure

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

KeyGen: The challenger \( \mathcal{C} \) picks a key \( k \leftarrow \mathcal{K}^{\text{SYM}} \)
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 \( b \leftarrow \{0, 1\} \) and responds with \( c \leftarrow \text{SYM.Enc}_k(m_b) \)
Guess: \( \mathcal{A} \) produces a bit \( b' \) and wins if \( b = b' \).
Formal Security Definitions
IND-CCA in QROM

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

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 $b \leftarrow \{0, 1\}$ 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 $G, H$. 