UNIVERSAL SECRET-KEY AND PUBLIC-KEY ENCRYPTION USING COMBINERS

A Thesis

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Master of Science

by

Olivia Eleftheria (Ellie) Fassman

May 2025

© 2025 Olivia Eleftheria (Ellie) Fassman

ALL RIGHTS RESERVED

UNIVERSAL SECRET-KEY AND PUBLIC-KEY ENCRYPTION USING COMBINERS

Olivia Eleftheria (Ellie) Fassman, M.S.

Cornell University 2025

We construct universal secret-key and public-key encryption schemes using combiners, in the style of Levin's universal one-way function. Given a finite list of candidate encryption schemes, our combiners produce a single scheme that is correct and semantically secure if and only if at least one of the input schemes satisfies these properties. Our constructions are efficient and require no assumptions beyond the existence of such a secure scheme within the list.

We develop and analyze these combiners for both the secret-key and public-key settings, establishing correctness and many-message semantic security. We show that if there exists any encryption scheme that is efficiently computable and semantically secure, then the output of our combiner is also secure and efficient. By enumerating all possible polynomial-time encryption schemes and applying our construction, we obtain universal encryption schemes which are secure if and only if any such scheme exists.

BIOGRAPHICAL SKETCH

Olivia Eleftheria (Ellie) Fassman received her Bachelor of Arts degree in Mathematics and Computer Science from Cornell University in 2023. In 2025, she completed her Master of Science degree in Computer Science at Cornell University, specializing in theoretical computer science. During her graduate studies, Ellie worked under the supervision of Dr. Noah Stephens-Davidowitz, focusing on theoretical cryptography. Ellie plans to continue her research in theoretical cryptography as she pursues a Ph.D. in Computer Science at the University of Michigan.

ACKNOWLEDGEMENTS

I am deeply grateful to my advisor, Dr. Noah Stephens-Davidowitz, for his guidance and support throughout this work. I also thank Dr. Anke van Zuylen, Dr. Robert Kleinberg, and Dr. Eshan Chattopadhyay for their support and encouragement along the way.

TABLE OF CONTENTS

CHAPTER 1

A COMBINER FOR SECRET-KEY ENCRYPTION SCHEMES

In this section, we present a simple way to convert ℓ secret-key encryption schemes $(\mathsf{Gen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i)_{i=1}^{\ell}$ (where ℓ might itself be a function of the security parameter n) into a single encryption scheme $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ so that $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is correct and secure if and only if there exists at least one i such that $(\mathsf{Gen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i)$ is correct and secure. The only assumption that we make is that the schemes $(\mathsf{Gen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i)$ are efficiently computable.

First, in order to ensure correctness, we will define simple modifications of the encryption schemes $(\mathsf{Gen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i)$, which we simply notate as $(\mathsf{Gen}'_i, \mathsf{Enc}'_i, \mathsf{Dec}'_i)$ for all $i \in \{1, \ldots, \ell\}$. The modified schemes behave as follows:

- $\mathsf{Gen}'_i(1^n) \coloneqq \mathsf{Gen}_i(1^n)$.
- $\mathsf{Enc}'_i(sk_i, m_i) \coloneqq$

  Compute $c_i \leftarrow \mathsf{Enc}_i(sk_i, m_i)$

  Check if $\mathsf{Dec}_i(sk_i, c_i) = m_i$

  If so, output $c'_i \coloneqq (1, c_i)$

  Otherwise, output $c'_i \coloneqq (0, m_i)$.
- $\mathsf{Dec}'_i(sk_i, (\alpha, c_i)) \coloneqq$

  Check if bit $\alpha = 1$

  If so, output $\mathsf{Dec}_i(sk_i, c_i)$

  Otherwise, output c_i.

We can now define how to combine these schemes as follows:

- $\mathsf{Gen}^*(1^n) \coloneqq$

  Output $sk^* \coloneqq (sk_1, \ldots, sk_\ell)$, where $sk_i \leftarrow \mathsf{Gen}'_i(1^n)$.

- $\mathsf{Enc}^*(sk^*, m \in \{0,1\}) \coloneqq$

  Flip ℓ coins $b_1, \ldots, b_\ell$

  Then for each b_i compute $c_i \leftarrow \mathsf{Enc}'_i(sk_i, b_i)$

  Let d be the XOR of these coins with the plaintext, that is, $d \coloneqq b_1 \oplus \ldots \oplus b_\ell \oplus m$

  Output $c^* \coloneqq (c_1, \ldots, c_\ell, d)$.

- $\mathsf{Dec}^*(sk^*, c^*) \coloneqq$

  For each $i \in [\ell]$, compute $b_i \leftarrow \mathsf{Dec}'_i(sk_i, c_i)$

  Output $b_1 \oplus \ldots \oplus b_\ell \oplus d$ which will result in the plaintext bit m.

CHAPTER 2

PROOF OF CORRECTNESS AND SECURITY

Theorem 2.0.1. $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ *is many message semantically secure and correct, assuming that at least one of the* ℓ *schemes is many message semantically secure and correct.*

Proof. For correctness, it is clear that $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is correct due to the use of $(\mathsf{Gen}'_i, \mathsf{Enc}'_i, \mathsf{Dec}'_i)$ for each i scheme. So all we need to show is security of $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$. If scheme i is many message semantically secure and correct, then so is $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$.

In order to prove this, we will show the contrapositive, that is that breaking $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ implies breaking the i scheme. Breaking $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ can be described by the figure below.

Definition of Many Message Semantic Security in the SKE Context

Adversary $(\mathcal{A})$		**Challenger** $(\mathcal{C})$
	$M_0 \in \{0,1\}^K, M_1 \in \{0,1\}^K \longrightarrow$	
		$sk \leftarrow \mathsf{Gen}^*(1^n)$
		$b \sim \{0,1\}$
		$c_i \leftarrow \mathsf{Enc}^*(sk, M_{b,[i]})$
	$\longleftarrow c_1, \ldots, c_K$	
	$b' \longrightarrow$	
		If $b = b'$, output WIN.

PPT adversary $\mathcal{A}$ wins, and thus breaks $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ if it is able to output the correct b' with probability non-negligibly larger than $\frac{1}{2}$. That is, with probability at least $\frac{1}{2} + \varepsilon(n)$ for some non-negligible $\varepsilon(n)$. Using this $\mathcal{A}$ we want to describe a PPT adversary $\mathcal{A}'$ that wins the many-message semantic security game against $\mathsf{Gen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i$ with probability at least $1/2 + \varepsilon(n)$. The behavior of $\mathcal{A}'$ can be described as follows:

Behavior of the Adversary in the SKE Context

$\mathcal{A}$	$\mathcal{A}'$	$\mathcal{C}'$
$M_0 \in \{0,1\}^K, M_1 \in \{0,1\}^K$ $\longrightarrow$		
	$B_0^i \sim \{0,1\}^K$ $B_1^i \sim \{0,1\}^K$	
	$\longrightarrow$ B_0^i, B_1^i	
		$sk_i \leftarrow \mathsf{Gen}'_i(1^n)$ $b^* \sim \{0,1\}$ $C^* \leftarrow \mathsf{Enc}'_i(sk_i, B_{b^*}^i)$
	$\longleftarrow$ C^*	
	$\mu \sim \{0,1\}$ For $j \in [\ell], j \neq i$: $sk_j \leftarrow \mathsf{Gen}'_j(1^n)$ $B_j \sim \{0,1\}^K$ $C_j \leftarrow \mathsf{Enc}'_j(sk_j, B_j)$ $B_i := B_0^i, C_i := C^*$ $D := B_1 \oplus \ldots \oplus B_\ell \oplus M_\mu$	
$(C_1, D_{[1]}), \ldots, (C_K, D_{[K]})$ $\longleftarrow$		
μ' $\longrightarrow$		
	If $\mu' = \mu, b' := 0$ Otherwise $b' := 1$	
	$\longrightarrow$ b'	
		If $b' = b^*$, output WIN.

$\mathcal{A}'$ arbitrarily assumed that $b^* = 0$. If, in fact, $b^* = 0$, then $\mathcal{A}$ has a non-negligible advantage at outputting μ' such that $\mu' = \mu$. That is, the probability that $\mu' = \mu$ given that $b^* = 0$ is at least $\frac{1}{2} + \varepsilon(n)$.

It is clear that if $b^* = 1$, $((C_1, D_{[1]}), \ldots, (C^*, D_{[*]}), \ldots, (C_K, D_{[K]}))$ is independent of μ, so the distribution of the ciphertext C^* is independent of μ. So in the case that $\mathcal{A}'$ was wrong in its assumption (that is, $b^* = 1$), $\mathcal{A}$ will receive $((C_1, D_{[1]}), \ldots, (C^*, D_{[*]}), \ldots, (C_K, D_{[K]}))$ where D is independent of this bit μ, and thus is independent of ciphertext C^*, meaning that the information that is revealed is independent of M_μ. Thus the probability of $\mathcal{A}$ outputting μ' such that $\mu' = \mu$ is exactly $\frac{1}{2}$.

Thus if $\mu' = \mu$ we say that $\mathcal{A}'$ was correct in its assumption that $b^* = 0$ and output $b' \coloneqq 0$. If $\mu' \neq \mu$ we say that $\mathcal{A}'$ was incorrect in its assumption and output $b' \coloneqq 1$. The probability that $\mathcal{A}'$ correctly outputs b' where $b' = b^*$ is at least $\frac{1}{2} + \frac{\varepsilon(n)}{2}$. Thus $\mathcal{A}'$ has a non-negligible advantage at breaking encryption scheme i since $\frac{\varepsilon(n)}{2}$ is non-negligible. So we see that $\mathcal{A}'$ breaks the security of $(\mathsf{Gen}'_i, \mathsf{Enc}'_i, \mathsf{Dec}'_i)$ given that $\mathcal{A}$ breaks the security of $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$. We have shown that if $(\mathsf{Gen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i)$ is secure for some $i \in \{1, \ldots, \ell\}$ then $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is secure. □

CHAPTER 3

UNIVERSAL SKE

We will modify the above to construct a universal secret key encryption scheme.

Fix an ordering $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1), (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2), \ldots, (\mathsf{Gen}_n, \mathsf{Enc}_n, \mathsf{Dec}_n)$ of secret key encryption schemes. We can use the notion of a combiner defined above for this ordering of schemes. That is, $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1), \ldots, (\mathsf{Gen}_n, \mathsf{Enc}_n, \mathsf{Dec}_n) \mapsto (\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$. We must consider the efficiency of these schemes in order to ensure that the combined scheme is efficiently computable. We will use efficiently computable and computable in polynomial time interchangeably, where computable in polynomial time means the asymptotic runtime is in $\mathcal{O}(n^C)$ for some constant C. The n input schemes are not necessarily computable in polynomial time, meaning they could run in superpolynomial time or could never halt. So to account for this we can limit each of the component schemes to run in at most $\mathcal{O}(n^2)$ time. This will ensure that the combined scheme $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is runs in $\mathcal{O}(n^3)$ time (n^3 since we have n schemes running in $\mathcal{O}(n^2)$ time).

Now say we have a correct and secure scheme $(\mathsf{Gen}(1^n), \mathsf{Enc}(sk, b), \mathsf{Dec}(sk, c))$ that runs in $\mathcal{O}(n^C)$ time (where C is a fixed constant). Then we can construct $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ where for $m \coloneqq n^{\frac{2}{C}}$, $\mathsf{Gen}^\dagger(1^n) \coloneqq \mathsf{Gen}(1^m), \mathsf{Enc}^\dagger(sk^\dagger, b^\dagger) \coloneqq \mathsf{Enc}(sk^\dagger, b^\dagger), \mathsf{Dec}^\dagger(sk^\dagger, c^\dagger) \coloneqq \mathsf{Dec}(sk^\dagger, c^\dagger)$.

Theorem 3.0.1. *If* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is correct and many message semantically secure, then* $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ *is also correct and many message semantically secure and runs in quadratic time.*

Proof. Correctness needs no proof since the encryption and decryption parts of $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ are identical to $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

To prove security, assume for the sake of contradiction that there exists some PPT $\mathcal{A}^\dagger$ and some non-negligible ε where the probability that $\mathcal{A}^\dagger$ correctly outputs the list of messages that was encrypted by $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ is non-negligibly better than guessing. That is, the probability that $\mathcal{A}^\dagger$ outputs $b^\dagger$ correctly is at least $\frac{1}{2} + \varepsilon(m)$. Quite simply we can use $\mathcal{A}^\dagger$ in our construction of PPT adversary $\mathcal{A}$ which attempts to break the security of $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. If $\mathcal{A}$ sends to challenger $\mathcal{C}$ the same bit $b^\dagger$ that $\mathcal{A}^\dagger$ outputs, then we can see that $\mathcal{A}$ has the same probability at breaking $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as $\mathcal{A}^\dagger$ does for $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$. Since $m = n^{\frac{2}{C}}$, we see that the advantage that $\mathcal{A}$ has in outputting the correct bit encrypted by $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is $\varepsilon(m)$ which is non-negligible if $\varepsilon(n)$ is non-negligible. Thus we see that if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ running in $\mathcal{O}(n^C)$ time is semantically secure then $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ running in $\mathcal{O}(n^2)$ time is also semantically secure. □

Thus we have shown that if there exists some secret key encryption scheme that is many message semantically secure and runs in polynomial time, then there exists an analogous scheme that runs in $\mathcal{O}(n^2)$ time. This ensures that for a scheme computable in polynomial time for a polynomial larger than n^2, we will not be altering the functionality of it when limiting each of the component schemes to run in at most $\mathcal{O}(n^2)$ time. Using the construction above (along with the proofs of correctness and security) we can say that if there exists some secret key encryption scheme that is many message semantically secure and runs in polynomial time, then the combined scheme $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is many message semantically secure and runs in $\mathcal{O}(n^3)$ time.

Theorem 3.0.2. $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ *is correct, many-message semantically secure, and computable in polynomial time if and only if there exists a correct and many-message semantically secure secret key encryption scheme computable in polynomial time.*

Proof. Through the specification of a combined scheme $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ from n component schemes, we have shown that as long as one of the component schemes is correct and secure, then the combined scheme is correct and secure. From here we can fix an ordering over all possible secret key encryption schemes that are computable in polynomial time. As proven above, we can convert any scheme running in polynomial time to an analogous scheme running in $\mathcal{O}(n^2)$ time.

So given an arbitrarily long but finite ordering over candidate secret key encryption schemes, these can be used as the input to the combined scheme. Since each component scheme can be converted to run in $\mathcal{O}(n^2)$ time, and we exhaustively enumerate through all possible schemes, the combined scheme will be computable in $\mathcal{O}(Ln^2)$ where L is the length of the arbitrarily long but finite list over all possible schemes. So as long as there exists a correct and many-message semantically secure scheme computable in polynomial time, which we will have in the order of all possible schemes, the combined scheme will be correct, many-message semantically secure, and computable in polynomial time. Note the that the reverse direction of the proof holds, that if the combined scheme is correct and many-message semantically secure, this is by definition one example of a correct and secure secret key encryption scheme.

□

Thus this combiner specifies a universal secret key encryption scheme.

CHAPTER 4

PKE COMBINER

In order to modify the construction of the secret key combiner to obtain a public key encryption, the only thing that needs to be modified is the $(\mathsf{Gen}'_i, \mathsf{Enc}'_i, \mathsf{Dec}'_i)$ for all $i \in [\ell]$. Once this is redefined, we can convert ℓ public key encryption schemes $(\mathsf{Gen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i)_{i=1}^{\ell}$ into a single public key encryption scheme $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ using the same behavior described in the secret key context. In order to ensure correctness, we can define $(\mathsf{Gen}'_i, \mathsf{Enc}'_i, \mathsf{Dec}'_i)$ as such:

- $\mathsf{Gen}'_i(1^n) \coloneqq$

  Compute $(pk_i, sk_i) \leftarrow \mathsf{Gen}_i(1^n)$

  For $j \in [n]$:

    Sample $b_j \sim \{0, 1\}$

    Compute $c_j \leftarrow \mathsf{Enc}_i(pk_i, b_j), b'_j \leftarrow \mathsf{Dec}_i(sk_i, c_j)$

    If $b_j \neq b'_j$, $f \leftarrow 1$

  If $f = 1$, output $(sk'_i, pk'_i) \coloneqq (0, 0)$

  Otherwise, output $(sk'_i, pk'_i) \coloneqq ((1, pk_i), (1, sk_i))$.

- $\mathsf{Enc}'_i(pk'_i, m_i) \coloneqq$

  If $pk_i = 0$, output $c' \coloneqq m_i$

  Otherwise for $j \in [n]$:

    Compute $c_j \leftarrow \mathsf{Enc}_i(pk_i, m_i)$

  Output $c' \coloneqq (c_1, \ldots, c_n)$.

- $\mathsf{Dec}'_i(sk'_i, c' \coloneqq (c_1, \ldots c_n)) \coloneqq$

  If $sk'_i = 0$, output c_1

  Otherwise for $j \in [n]$:

  Compute $b_j \leftarrow \mathsf{Dec}_i(sk'_i, c_j)$

  Output $\mathsf{maj}(b_1, \ldots, b_n)$.

We can now define how to combine these schemes as follows:

- $\mathsf{Gen}^*(1^n) \coloneqq$

  For $i \in [\ell]$:

  Compute $(pk_i, sk_i) \leftarrow \mathsf{Gen}'_i(1^n)$

  Output $(pk^*, sk^*) := ((pk_1, sk_1), \ldots, (pk_\ell, sk_\ell))$.

- $\mathsf{Enc}^*(pk^*, m \in \{0,1\}) \coloneqq$

  Flip ℓ coins $b_1, \ldots, b_\ell$

  Then for each b_i, compute $c_i \leftarrow \mathsf{Enc}'_i(pk_i, b_i)$

  Compute $d := b_1 \oplus \ldots \oplus b_\ell \oplus m$

  Output $c^* := (c_1, \ldots, c_\ell, d)$.

- $\mathsf{Dec}^*(sk^*, c^* \coloneqq (c_1, \ldots, c_\ell, d)) \coloneqq$

  For each $i \in [\ell]$, compute $b_i \leftarrow \mathsf{Dec}'_i(sk_i, c_i)$

  Output $b_1 \oplus \ldots \oplus b_\ell \oplus d$, which will result in the plaintext bit m.

CHAPTER 5

PROOF OF CORRECTNESS AND SECURITY

Theorem 5.0.1. $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ *is a correct public key encryption scheme*

Proof. First we must show that $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is a correct public key encryption scheme. We defined $(\mathsf{Gen}'_i, \mathsf{Enc}'_i, \mathsf{Dec}'_i)$ for each i in order to ensure correctness of the combined scheme. In the definition of the key generation algorithm Gen'_i, if scheme i incorrectly decrypts a bit at least once in n trials, then the scheme is not used and the plaintext m_i is sent in the clear.

So if a scheme k decrypts incorrectly with probability at least $\frac{1}{10}$, then the probability that this scheme it will decrypt all n trials correctly is at most $(\frac{9}{10})^n$, which is a negligible function. So for reasonably large n (which is the security parameter), the probability that scheme k incorrectly decrypts at least once is at least $1 - (\frac{9}{10})^n$, where $(\frac{9}{10})^n$ is a negligible function. With negligible probability the key generation algorithm fails to catch incorrectly decrypting scheme k, so with probability negligibly close to 1, the key generation algorithm succeeds in catching scheme k and sends the plaintext in the clear.

We can also see that if $(\mathsf{Gen}_k, \mathsf{Enc}_k, \mathsf{Dec}_k)$ decrypts incorrectly with probability less than $\frac{1}{10}$, then the probability that each bit is decrypted correctly is at least $\frac{9}{10}$. In taking the majority over n bits, where decryption of the original scheme has an error of less than $\frac{1}{10}$, we can bound the probability that $(\mathsf{Gen}'_k, \mathsf{Enc}'_k, \mathsf{Dec}'_k)$ decrypts incorrectly.

Let X_j be the indicator variable representing the jth time decrypting a bit. $X_j = 1$ if this jth decryption returns the incorrect result. So $X = \Sigma_{j=1}^{n} X_j$ is the random variable representing the number of times scheme k decrypts incorrectly. So we have that $\mathbb{E}[X] = \frac{1}{10}n$. The probability of outputting the wrong bit when taking the majority over n decrypted bits is at most $\Pr[X \geq \frac{n}{2}]$. $\Pr[X \geq \frac{n}{2}] = \Pr[X \geq (1 + \frac{1}{2})\frac{n}{3}]$ and we see that $\mathbb{E}[X] \leq \frac{n}{3}$. So using

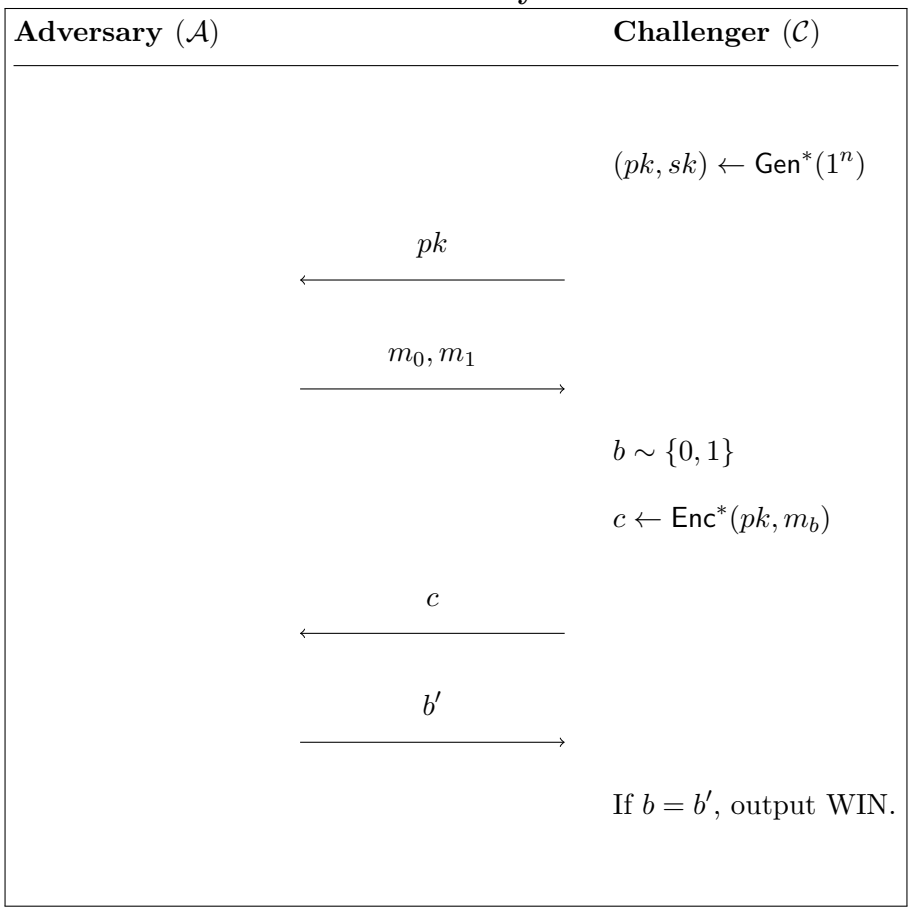
the Chernoff bound we get $\Pr[X \geq (1+\frac{1}{2})\frac{n}{3}] \leq e^{\frac{-n}{36}}$, which is a negligible function. So the probability of outputting the wrong bit for this scheme k is bounded above by a negligible function.

Thus $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is correct due to the use of $(\mathsf{Gen}'_i, \mathsf{Enc}'_i, \mathsf{Dec}'_i)$ for each i scheme in the list of ℓ public key encryption schemes. □

Theorem 5.0.2. $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ *is semantically secure and correct, assuming that at least one of the* ℓ *schemes is semantically secure and correct.*

Proof. Now to show the security of $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$. For PKE, we must show is that if scheme i is single message semantically secure and correct, then so is $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$. In order to prove this, we will show the contrapositive, that is that breaking $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ implies breaking the i scheme. Breaking $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ means there exists some PPT $\mathcal{A}$ and some non-negligible ε where the probability that $\mathcal{A}$ correctly outputs the bit that was encrypted by $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is non-negligibly better than guessing. That is, the probability that $b' = b$ is at least $\frac{1}{2} + \varepsilon(n)$. Breaking $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ can be described by the figure below.

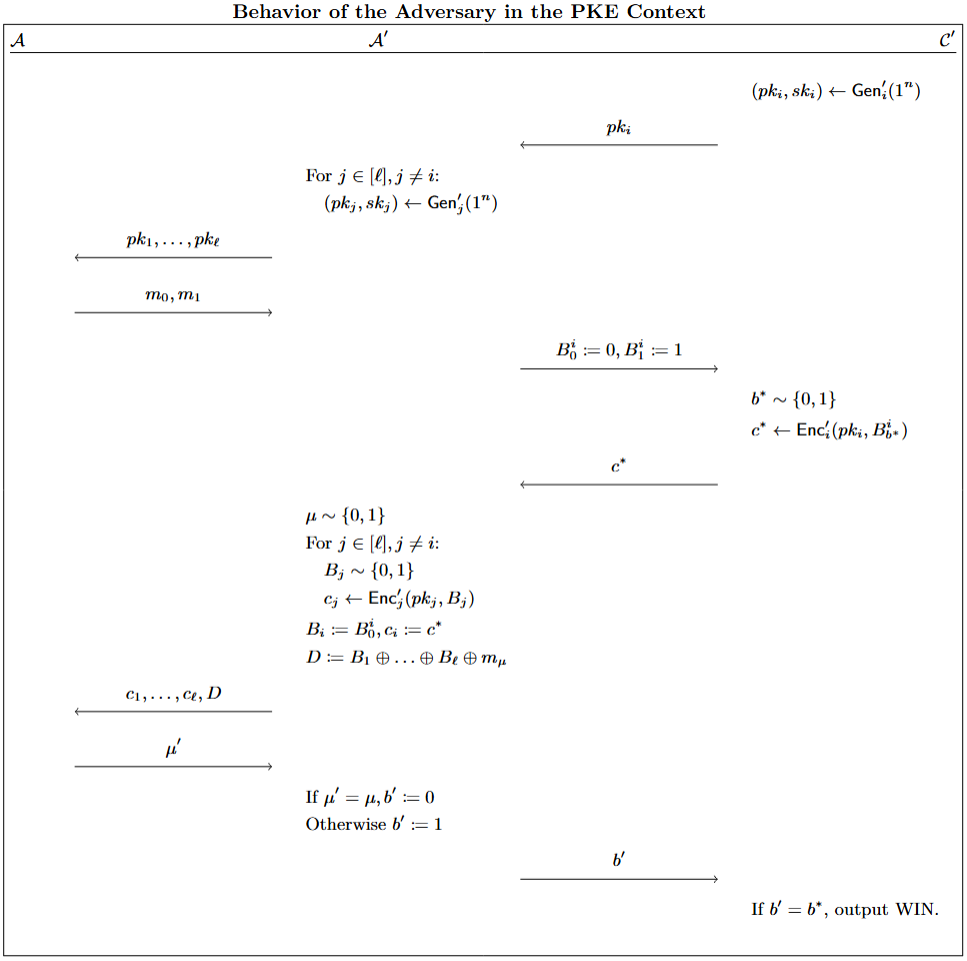
Definition of Semantic Security in the PKE Context



Using this $\mathcal{A}$ we want to describe a PPT adversary $\mathcal{A}'$ that wins the semantic security game against $\mathsf{Gen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i$ with probability at least $\frac{1}{2} + \varepsilon(n)$. The behavior of $\mathcal{A}'$ can be described as follows:

(Note that the behavior of $\mathcal{A}'$ is the same as in the secret key context, with two modifications. The first is that $K = 1$ since we only need to show single message semantic security. Secondly, we are working with public keys, so in the security game the challenger $\mathcal{C}'$ sends to $\mathcal{A}'$ the i^{th} public key, pk_i and $\mathcal{A}'$ sends to $\mathcal{A}$ the list of public keys, $pk_1, \ldots, pk_\ell$.)

Behavior of the Adversary in the PKE Context



$\mathcal{A}'$ arbitrarily assumed that $b^* = 0$. If, in fact, $b^* = 0$, then $\mathcal{A}$ has a non-negligible advantage at outputting μ' such that $\mu' = \mu$. That is, the probability that $\mathcal{A}$ outputs the correct μ' given that $b^* = 0$ is at least $\frac{1}{2} + \varepsilon(n)$.

It is clear that if $b^* = 1$, $(c_1, \ldots, c^*, \ldots, c_\ell, D)$ is independent of μ, so the distribution of the ciphertext c^* is independent of μ. So in the case that $\mathcal{A}'$ was wrong in its assumption (that is, $b^* = 1$), $\mathcal{A}$ will receive $(c_1, \ldots, c^*, \ldots, c_\ell, D)$ where D is independent of this bit μ, and thus is independent of ciphertext c^*, meaning that the information that is revealed is independent of M_μ. Thus the probability that $\mu' = \mu$ is exactly $\frac{1}{2}$.

Thus if $\mu' = \mu$ we say that $\mathcal{A}'$ was correct in its assumption that $b^* = 0$ and if $\mu' \neq \mu$ we say that $\mathcal{A}'$ was incorrect in its assumption and $b^* = 1$. The probability that $b' = b^*$ is at least $\frac{1}{2} + \frac{\varepsilon(n)}{2}$ since $\mathcal{A}$ only has a non-negligible advantage at outputting the correct μ' when $b^* = 0$. Since b^* is a randomly sampled bit, this happens with probability exactly $\frac{1}{2}$. So $\mathcal{A}'$ has a non-negligible advantage at breaking encryption scheme i since $\frac{\varepsilon(n)}{2}$ is non negligible. So we see that $\mathcal{A}'$ breaks the security of $(\mathsf{Gen}'_i, \mathsf{Enc}'_i, \mathsf{Dec}'_i)$ given that $\mathcal{A}$ breaks the security of $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$. We have shown that if $(\mathsf{Gen}_i, \mathsf{Enc}_i, \mathsf{Dec}_i)$ is secure for some $i \in \{1, \ldots, \ell\}$ then $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is secure. □

CHAPTER 6

UNIVERSAL PKE

We will generalize what is above to construct a universal public key encryption scheme.

Fix an ordering $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1), (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2), \ldots, (\mathsf{Gen}_n, \mathsf{Enc}_n, \mathsf{Dec}_n)$ of public key encryption schemes. We can use the notion of a combiner defined above for this ordering of schemes. That is, $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1), \ldots, (\mathsf{Gen}_n, \mathsf{Enc}_n, \mathsf{Dec}_n) \mapsto (\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$. We must consider the efficiency of these schemes in order to ensure that the combined scheme is efficiently computable. The n input schemes are not necessarily computable in polynomial time, meaning they could run in superpolynomial time or could never halt. So to account for this we can limit each of the component schemes to run in at most $\mathcal{O}(n^2)$ time. This will ensure that the combined scheme $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is runs in $\mathcal{O}(n^3)$ time (n^3 since we have n schemes running in $\mathcal{O}(n^2)$ time).

Say we have a correct and secure scheme $(\mathsf{Gen}(1^n), \mathsf{Enc}(pk, b), \mathsf{Dec}(sk, c))$ that runs in $\mathcal{O}(n^C)$ time. Then we can construct $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ where for $m \coloneqq n^{\frac{2}{C}}$, $\mathsf{Gen}^\dagger(1^n) \coloneqq \mathsf{Gen}(1^m), \mathsf{Enc}^\dagger(pk^\dagger, b^\dagger) \coloneqq \mathsf{Enc}(pk^\dagger, b^\dagger), \mathsf{Dec}^\dagger(sk^\dagger, c^\dagger) \coloneqq \mathsf{Dec}(sk^\dagger, c^\dagger)$.

Theorem 6.0.1. *If* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is correct and semantically secure, then* $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ *is also correct and semantically secure and runs in quadratic time.*

Proof. Correctness needs no proof since the encryption and decryption parts of $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ are identical to $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

To prove security, assume for the sake of contradiction that there exists some PPT $\mathcal{A}^\dagger$ and some non-negligible ε where the probability that $\mathcal{A}^\dagger$ correctly outputs the message that was encrypted by $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ is non-negligibly better than guessing. That is, the

probability that $\mathcal{A}^\dagger$ outputs $b^\dagger$ correctly is at least $\frac{1}{2} + \varepsilon(m)$. Quite simply we can use $\mathcal{A}^\dagger$ in our construction of PPT adversary $\mathcal{A}$ which attempts to break the security of $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. If $\mathcal{A}$ sends to challenger $\mathcal{C}$ the same bit $b^\dagger$ that $\mathcal{A}^\dagger$ outputs, then we can see that $\mathcal{A}$ has the same probability at breaking $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as $\mathcal{A}^\dagger$ does for $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$. Since $m = n^{\frac{2}{C}}$, we see that the advantage that $\mathcal{A}$ has in outputting the correct bit encrypted by $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is $\varepsilon(m)$ which is non-negligible if $\varepsilon(n)$ is non-negligible. Thus we see that if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ running in $\mathcal{O}(n^C)$ time is semantically secure then $(\mathsf{Gen}^\dagger, \mathsf{Enc}^\dagger, \mathsf{Dec}^\dagger)$ running in $\mathcal{O}(n^2)$ time is also semantically secure. □

Thus we have shown that if there exists some public key encryption scheme that is semantically secure and runs in polynomial time, then there exists an analogous scheme that runs in $\mathcal{O}(n^2)$ time. This ensures that for a scheme computable in non-quadratic polynomial time, we will not be altering the functionality of it when limiting each of the component schemes to run in at most $\mathcal{O}(n^2)$ time. Using the construction above we can say that if there exists some public key encryption scheme that is semantically secure and runs in polynomial time, then the combined scheme $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ is secure and runs in $\mathcal{O}(n^3)$ time.

Theorem 6.0.2. $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ *is correct, semantically secure, and computable in polynomial time if and only if there exists a correct and semantically secure public key encryption scheme computable in polynomial time.*

Proof. Through the specification of a combined scheme $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$ from n component schemes, we have shown that as long as one of the component schemes is correct and secure, then the combined scheme is correct and secure. From here we can fix an ordering over all possible public key encryption schemes that are computable in polynomial time. As proven above, we can convert any scheme running in polynomial time to an analogous scheme running in $\mathcal{O}(n^2)$ time.

So given an arbitrarily long but finite ordering over candidate public key encryption schemes, these can be used as the input to the combined scheme. Since each component scheme can be converted to run in $\mathcal{O}(n^2)$ time, and we exhaustively enumerate through all possible schemes, the combined scheme will be computable in $\mathcal{O}(Ln^2)$ where L is the length of the arbitrarily long but finite list over all possible schemes. So as long as there exists a correct and semantically secure scheme computable in polynomial time, which we will have in the order of all possible schemes, the combined scheme will be correct, semantically secure, and computable in polynomial time. Note the that the reverse direction of the proof holds, that if the combined scheme is correct and semantically secure, this is by definition one example of a correct and secure public key encryption scheme. □

Thus this combiner specifies a universal public key encryption scheme.

BIBLIOGRAPHY

[1] Leonid A. Levin. One way functions and pseudorandom generators. *Combinatorica*, 7(4):357–363, December 1987.

[2] Leonid A. Levin. The tale of one-way functions. *Problems of Information Transmission*, 39(1):92–103, January 2003.