1 Preliminaries

1.1 Plaintext awareness

Plaintext awareness (PA)[BR95, BDPR98] describes the idea that no efficient algorithm can produce a valid ciphertext without knowing the corresponding decryption.

Let $\mathtt{PKE} = (\mathtt{KeyGen}, \mathtt{E}, \mathtt{D})$ be a public-key encryption scheme. Let H be a hash function. Let $\mathcal{E}^H_{\mathtt{pk}}$ be an encryption oracle that takes no argument and returns valid ciphertexts when queried. Under the random oracle model, hash queries made to the oracle $\mathcal{O}^H$ can be logged to a tape $\mathcal{L}^H = \{(h_i, H(h_i))\}$, and ciphertexts obtained from the encryption oracle are also logged to a separate tape $C = \{c : c \leftarrow \mathcal{E}^H_{\mathtt{pk}}(\cdot)\}$.

A plaintext-awareness adversary B is a probabilistic algorithm that is given some public key and access to the two oracles, then output some ciphertext c. Note that the encryption oracle here is not redundant because obtaining ciphertexts from the encryption oracle will not log any corresponding hash queries in the hash oracle. This models a PA adversary's ability to obtain valid ciphertexts without running the encryption routine, such as by eavesdropping. The PA adversary B outputs a ciphertext c and the transcript $\mathcal{L}^H, C$ of its interactions with the oracles.

Let K be some algorithm that outputs a decryption of c using the corresponding transcript $\mathcal{L}^H, C$. We restrict $c \notin C$ to prevent trivially turning K into a decryption oracle. The plaintext awareness game is defined in figure 1.

Algorithm 1 Plaintext awareness game

1: $(\mathtt{pk}, \mathtt{sk}) \xleftarrow{\$} \mathtt{KeyGen}(1^\lambda)$
2: $(\mathcal{L}^H, C, c) \leftarrow B^{H, \mathcal{E}^H_{\mathtt{pk}}}(1^\lambda, \mathtt{pk})$
3: $m \leftarrow K(1^\lambda, \mathtt{pk}, \mathcal{L}^H, C, c)$
4: **return** $[\![c \notin C \wedge m = D(\mathtt{sk}, c)]\!]$

Figure 1: The plaintext awareness game

Definition 1.1. *A public-key encryption scheme is* plaintext-aware *if there exists an efficient K such that for all efficient PA adversaries B, the probability of K failing to extract the correct decryption is negligible.*

$$P[\mathtt{PA(K,\ B)} \neq 1] \leq \mathtt{negl}(\lambda)$$

Note that our definition of plaintext awareness deviates from [BDPR98] in that we do not require the $\mathtt{PKE}$ to also be IND-CPA secure. This is because in constructing a key encapsulation mechanism using the Fujisaki-Okamoto transformation, we only require the input $\mathtt{PKE}$ to be one-way secure, though under a stronger attack model. Restricting the definition to only the plaintext-awareness game allows us to combine PA with other security definition, such as OW-CPA, to prove stronger security result.

2 Encrypt-then-MAC transformations

Let $\mathtt{PKE}(\mathtt{KeyGen}, \mathtt{E}, \mathtt{D})$ be a probabilistic public-key encryption scheme defined over message space $\mathcal{M}_{\mathtt{PKE}}$, ciphertext space $\mathcal{C}_{\mathtt{PKE}}$, and coin space $\mathcal{R}_{\mathtt{PKE}}$. Where the encryption routine is deterministic, we simply set the coin space to contain a single element $\mathcal{R} = \{r\}$. Let $\mathtt{MAC}(\mathtt{Sign}, \mathtt{Verify})$ be a message authentication code defined over key space $\mathcal{K}_{\mathtt{MAC}}$. The message space of the $\mathtt{MAC}$ should contain the ciphertext space of the $\mathtt{PKE}$: $\mathcal{C}_{\mathtt{PKE}} \subseteq \mathcal{M}_{\mathtt{MAC}}$. Let $G : \mathcal{M}_{\mathtt{PKE}} \to \mathcal{R}_{\mathtt{PKE}}$ and $H : \mathcal{M}_{\mathtt{PKE}} \to \mathcal{K}_{\mathtt{MAC}}$ be hash functions.

The "encrypt-then-MAC" transformation $\mathtt{PKE}_{\mathtt{EtM}}(\mathtt{KeyGen}, \mathtt{E}_{\mathtt{EtM}}, \mathtt{D}_{\mathtt{EtM}}) = T_{\mathtt{EtM}}(\mathtt{PKE}, \mathtt{MAC}, H)$ outputs a public-key encryption scheme where the key generation routine is identical to the input $\mathtt{PKE}$'s key generation routine. The de-randomized "encrypt-then-MAC" transformation $\mathtt{PKE}^{\$}_{\mathtt{EtM}}(\mathtt{KeyGen}, \mathtt{E}^{\$}_{\mathtt{EtM}}, \mathtt{D}^{\$}_{\mathtt{EtM}}) = T^{\$}_{\mathtt{EtM}}(\mathtt{PKE}, \mathtt{MAC}, G, H)$ similarly outputs a public-key encryption scheme. In both transformations, the key generation routine remains unchanged. The modified encryption and decryption routines are described in figure 2 and 3.

Algorithm 2 $\mathtt{E}_{\mathtt{EtM}}(\mathtt{pk}, m)$

$r \xleftarrow{\$} \mathcal{R}_{\mathtt{PKE}}$ $\quad\triangleright$ If $\mathtt{E}$ is randomized, then $\mathtt{E}_{\mathtt{EtM}}$ is randomized
$k_{\mathtt{MAC}} \leftarrow H(m)$
$c \leftarrow \mathtt{E}(\mathtt{pk}, m; r)$
$t \leftarrow \mathtt{Sign}(k_{\mathtt{MAC}}, c)$
return (c, t)

Algorithm 3 $\mathtt{D}_{\mathtt{EtM}}(\mathtt{sk}, (c, t))$

$\hat{m} \leftarrow \mathtt{D}(\mathtt{sk}, c)$
$\hat{k}_{\mathtt{MAC}} \leftarrow G(\hat{m})$
if $\mathtt{Verify}(\hat{k}_{\mathtt{MAC}}, c, t) \neq 1$ **then**
  return $\perp$
end if
return $\hat{m}$

Figure 2: "encrypt-then-MAC" transformation

Algorithm 4 $\mathtt{E}^{\not\$}_{\mathtt{EtM}}(\mathtt{pk}, m)$

$k_{\mathtt{MAC}} \leftarrow H(m)$
$r \leftarrow G(m)$
$c \leftarrow \mathtt{E}(\mathtt{pk}, m; r)$
$t \leftarrow \mathtt{Sign}(k_{\mathtt{MAC}}, c)$
return (c, t)

Algorithm 5 $\mathtt{D}^{\not\$}_{\mathtt{EtM}}(\mathtt{sk}, (c, t))$

$\hat{m} \leftarrow \mathtt{D}(\mathtt{sk}, c)$
$\hat{k}_{\mathtt{MAC}} \leftarrow G(\hat{m})$
if $\mathtt{Verify}(\hat{k}_{\mathtt{MAC}}, c, t) \neq 1$ **then**
  return $\perp$
end if
return $\hat{m}$

Figure 3: de-randomized "encrypt-then-MAC" transformation

References

[BDPR98] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology—CRYPTO'98: 18th Annual International Cryptology Conference Santa Barbara, California, USA August 23–27, 1998 Proceedings 18*, pages 26–45. Springer, 1998.

[BR95] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In *Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings 13*, pages 92–111. Springer, 1995.