The "encrypt-then-MAC" transformations

Ganyu (Bruce) Xu (g66xu)

June 26, 2024

1 Encrypt-then-MAC transformations

In this section we describe two "encrypt-then-MAC" transformations and discuss their security properties.

Algorithm 1 $\mathtt{E}_{\mathtt{EtM}}(\mathtt{pk}, m)$

$k_{\mathtt{MAC}} \leftarrow G(m)$
$c \leftarrow \mathtt{E}(\mathtt{pk}, m)$ ▷ If $\mathtt{E}$ is randomized, then $\mathtt{E}_{\mathtt{EtM}}$ is randomized
$t \leftarrow \mathtt{Sign}(k_{\mathtt{MAC}}, c)$
return (c, t)

Algorithm 2 $\mathtt{D}_{\mathtt{EtM}}(\mathtt{sk}, (c, t))$

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

Figure 1: EtM transformation.

Algorithm 3 $\mathtt{E}^{\$}_{\mathtt{EtM}}(\mathtt{pk}, m)$

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

Algorithm 4 $\mathtt{D}^{\$}_{\mathtt{EtM}}(\mathtt{sk}, (c, t))$

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

Figure 2: Derandomized encrypt-then-MAC

Algorithm 5 Sequence of games

$(\mathtt{pk}, sk) \xleftarrow{\$} \mathtt{KeyGen}(1^\lambda)$
$m^* \xleftarrow{\$} \mathcal{M}_{\mathtt{PKE}}$
$k^*_{\mathtt{MAC}} \leftarrow H(m^*)$ ▷ Game 0-2
$k^*_{\mathtt{MAC}} \xleftarrow{\$} \mathcal{K}_{\mathtt{MAC}}$ ▷ Game 3
$c^* \xleftarrow{\$} \mathtt{E}(\mathtt{pk}, m)$
$t^* \leftarrow \mathtt{Sign}(k^*_{\mathtt{MAC}}, c^*)$
$\hat{m} \leftarrow \mathcal{A}^{\mathtt{PCO},\mathtt{CVO},\mathcal{O}^H}(1^\lambda, \mathtt{pk}, (c^*, t^*))$ ▷ Game 0
$\hat{m} \leftarrow \mathcal{A}^{\mathtt{PCO}_1,\mathtt{CVO},\mathcal{O}^H}(1^\lambda, \mathtt{pk}, (c^*, t^*))$ ▷ Game 1
$\hat{m} \leftarrow \mathcal{A}^{\mathtt{PCO}_1,\mathtt{CVO}_1,\mathcal{O}^H}(1^\lambda, \mathtt{pk}, (c^*, t^*))$ ▷ Game 2-3
return $[\![\hat{m} = m^*]\!]$

Figure 3: Sequence of games 0-3

Algorithm 6 $\mathtt{PCO}(m, (c, t))$

$\hat{m} \leftarrow \mathtt{D}(\mathtt{sk}, c)$
$\hat{k}_{\mathtt{MAC}} \leftarrow H(\hat{m})$
if $\mathtt{Sign}(\hat{k}_{\mathtt{MAC}}, c) \neq t$ **then**
    return 0
end if
return $[\![\hat{m} = m]\!]$

Algorithm 7 $\mathtt{PCO}_1(m, (c, t))$

if $\exists(\tilde{m}, \tilde{k}) \in \mathcal{O}^H : \tilde{m} = m \wedge \mathtt{Sign}(\tilde{k}, c) = t$ **then**
    return 1
end if
return 0

Figure 4: True $\mathtt{PCO}$ and simulated $\mathtt{PCO}$

Algorithm 8 $\mathtt{CVO}(c, t)$

$\hat{m} \leftarrow \mathtt{D}(\mathtt{sk}, c)$
$\hat{k}_{\mathtt{MAC}} \leftarrow H(\hat{m})$
if $\mathtt{Sign}(\hat{k}_{\mathtt{MAC}}, c) \neq t$ **then**
    return 0
end if
return 1

Algorithm 9 $\mathtt{CVO}_1(c, t)$

if $\exists(\tilde{m}, \tilde{k}) \in \mathcal{O}^H : \mathtt{Sign}(\tilde{k}, c) = t$ **then**
    return 1
end if
return 0

Figure 5: True $\mathtt{CVO}$ and simulated $\mathtt{CVO}_1$