Chosen-Ciphertext Security (II)

CS 601.442/642 Modern Cryptography

Fall 2018
Recall: Chosen-Ciphertext Attacks (CCA)

- Adversary can make decryption queries over ciphertext of its choice
- **CCA-1**: Decryption queries only before challenge ciphertext query
- **CCA-2**: Decryption queries before and after challenge ciphertext query
- No decryption query \( c \) should be equal to challenge ciphertext \( c^* \)

**Last time**: Construction of CCA-1 secure PKE

**Today**: Construction of CCA-2 secure PKE
Recall: CCA-2 Security

\(\text{Expt}^{\text{CCA2}}_A(b, z)\):

- \(\text{st} = z\)
- \((pk, sk) \leftarrow \text{Gen}(1^n)\)
- **Decryption query phase 1 (repeated poly times):**
  - \(c \leftarrow A(pk, \text{st})\)
  - \(m \leftarrow \text{Dec}(sk, c)\)
  - \(\text{st} = (\text{st}, m)\)
- \((m_0, m_1) \leftarrow A(pk, \text{st})\)
- \(c^* \leftarrow \text{Enc}(pk, m_b)\)
- **Decryption query phase 2 (repeated poly times):**
  - \(c \leftarrow A(pk, c^*, \text{st})\)
  - If \(c = c^*\), output reject
  - \(m \leftarrow \text{Dec}(sk, c)\)
  - \(\text{st} = (\text{st}, m)\)
- Output \(b' \leftarrow A(pk, c^*, \text{st})\)
Definition (IND-CCA-2 Security)

A public-key encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) is IND-CCA-2 secure if for all n.u. PPT adversaries \(A\), there exists a negligible function \(\mu(\cdot)\) s.t. for all auxiliary inputs \(z \in \{0, 1\}^*\):

\[
\left| \Pr \left[ \text{Expt}_{A}^{\text{CCA2}}(1, z) = 1 \right] - \Pr \left[ \text{Expt}_{A}^{\text{CCA2}}(0, z) = 1 \right] \right| \leq \mu(n)
\]
How to Construct CCA-2 secure Encryption?

- Why doesn’t a CCA-1 secure scheme also achieve CCA-2 security?

- **Main problem:** An adversary may be able to modify the challenge ciphertext to obtain a new ciphertext of a related plaintext and then request its decryption in the second decryption query phase of IND-CCA-2. E.g., the adversary may be able to “maul” an encryption of $x$ into an encryption of $x \oplus 1$ without knowing $x$. This is called *malleability attack*.

  **Think:** Is the IND-CPA PKE scheme based on trapdoor permutations that we studied in the class *malleable*?

- **Solution Strategy:** Ensure that adversary’s decryption query is “independent” of (and not just different from) the challenge ciphertext. That is, make the encryption *non-malleable*.
The first construction of CCA-2 secure encryption scheme was given by Dolev-Dwork-Naor.

**Ingredients:**

- An IND-CPA secure encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\)
- A NIZK proof \((P, V)\) (for simplicity of notation, we use NIZK in Random oracle model, but the construction also works if we use NIZKs in CRS model)
- A strongly unforgeable one-time signature (OTS) scheme \((\text{Setup}, \text{Sign}, \text{Verify})\). Assume, wlog, that verification keys in OTS scheme are of length \(n\).
Construction of \((\text{Gen}'', \text{Enc}'', \text{Dec}'')\):

\textbf{Gen}'\, (1^n)\: \text{Execute the following steps}

- Compute \(2n\) key pairs of IND-CPA encryption scheme: \((pk^j_i, sk^j_i) \leftarrow \text{Gen}(1^n), \text{where } j \in \{0, 1\}, i \in [n].\)
- Output \(pk' = (\{pk^0_i, pk^1_i\}), \ sk' = (sk^0_1, sk^1_1).\)
Construction (contd.)

\( \text{Enc}'(pk', m) \): Execute the following steps

- Compute key pair for OTS scheme:
  \( (SK, VK) \leftarrow \text{Setup}(1^n) \).
- Let \( VK = VK_1, \ldots, VK_n \). For every \( i \in [n] \), encrypt \( m \) using \( pk'_iVK_i \) and randomness \( r_i \):
  \[ c_i \leftarrow \text{Enc}(pk'_iVK_i, m; r_i) \]
- Compute proof that each \( c_i \) encrypts the same message:
  \( \pi \leftarrow P(x, w) \) where \( x = \left( \left\{ pk'_iVK_i \right\}, \{ c_i \} \right) \),
  \( w = (m, \{ r_i \}) \) and \( R(x, w) = 1 \) iff every \( c_i \) encrypts the same message \( m \).
- Sign everything:
  \( \Phi \leftarrow \text{Sign}(SK, M) \) where
  \( M = (\{ c_i \}, \pi) \)
- Output \( c' = (VK, \{ c_i \}, \pi, \Phi) \)
Dec′(sk′, c′): Execute the following steps

- Parse $c′ = (VK, \{c_i\}, \pi, \Phi)$
- Let $M = (\{c_i\}, \pi)$
- Verify the signature: Output ⊥ if
  Verify $(VK, M, \Phi) = 0$
- Verify the NIZK proof: Output ⊥ if $V(x, \pi) = 0$
  where $x = \left(\left\{ pk_i^{VK_i} \right\}, \{c_i\}\right)$
- Else, decrypt the first ciphertext component:
  $m' \leftarrow \text{Dec}\left(sk_1^{VK_1}, c_1\right)$
- Output $m'$
Consider decryption queries after adversary receives challenge ciphertext $C^*$:

- Let $C \neq C^*$ be a decryption query
- If verification key $VK$ in $C$ and verification key $VK^*$ in challenge ciphertext $C^*$ are same, then we can break the strong unforgeability of OTS
- If different, then $VK$ and $VK^*$ differ in at least one position $\ell \in [n]$:  
  - Answer decryption query using the secret key $sk^V_{\ell K_i}$.
  - Don’t need to know the secret keys $sk^V_{i K_i^*}$ for $i \in [n]$
  - Reduce to IND-CPA security of underlying encryption scheme
Security (Hybrids)

- $H_0$: (Honest) Encryption of $m_0$
- $H_1$: Compute proof $\pi$ in challenge ciphertext using NIZK simulator
- $H_2$: Choose $VK^*$ in the beginning during $Gen'$
- $H_3$: For any decryption query $C = (VK, \{c_i\}, \pi, \Phi)$:
  - If $VK = VK^*$ and $Verify(VK, (\{c_i\}, \pi), \Phi) = 1$, then abort
  - Else, let $\ell \in [n]$ be such that $VK^*$ and $VK$ in $c$ differ at position $\ell$. Set $sk' = \left\{ sk_i^{VK^*} \right\}$, $i \in [n]$, where $VK^*_i = 1 - VK^*_i$. Decrypt $c$ by decrypting $c_\ell$ (instead of $c_1$) using $sk_\ell^{VK^*_\ell}$.
- $H_4$: Change every $c_i^*$ in $C^*$ to encryption of $m_1$
- $H_5$: Compute proof $\pi$ in challenge ciphertext honestly. This experiment is same as (honest) encryption of $m_1$. 
Indistinguishability of Hybrids

- $H_0 \approx H_1$: ZK property of NIZK
- $H_1 \approx H_2$: Generating $VK^*$ early or later does not change the distribution
- $H_2 \approx H_3$: We argue indistinguishability as follows:
  - First, we argue that probability of aborting is negligible. Recall that $c \neq c^*$ by the definition of CCA-2. Then, if $VK = VK^*$, it must be that $(\{c_i\}, \pi, \Phi) \neq (\{c_i^*\}, \pi^*, \Phi^*)$. Now, if $\text{Verify}(VK, (\{c_i\}, \pi), \Phi) = 1$, then we can break strong unforgeability of the OTS scheme.
  - Now, conditioned on not aborting, let $\ell$ be the position s.t. $VK_\ell \neq VK^*_\ell$. Note that the only difference in $H_2$ and $H_3$ in this case might be the answers to the decryption queries of adversary. In particular, in $H_2$, we decrypt $c_1$ in $c$ using $sk_1^{VK_1}$. In contrast, in $H_3$, we decrypt $c_\ell$ in $c$ using $sk_\ell^{VK^*_\ell}$. Now, from soundness of NIZK, it follows that except with negligible probability, all the $c_i$’s in $c$ encrypt the same message. Therefore decrypting $c_\ell$ instead of $c_1$ does not change the answer.
\[ \begin{align*}
& \bullet \ H_3 \approx H_4: \text{IND-CPA security of underlying PKE} \\
& \bullet \ H_4 \approx H_5: \text{ZK property of NIZK} \\
\text{Combining the above, we get } & H_0 \approx H_5. \\
\end{align*} \]