Relaxing IND-CCA: Indistinguishability Against Chosen Ciphertext Verification Attack

Sumit Kumar Pandey, Santanu Sarkar and Mahavir Prasad Jhanwar

CR Rao AIMSCS
Hyderabad

November 2, 2012

Outline

1. Definitions
   - Encryption Scheme
   - IND-CPA
   - IND-CCA
   - IND-CCVA
2. Bleichenbacher's attack on PKCS#1
3. Generic Constructions

Definition: Encryption Scheme

- **KG(1^λ):** A probabilistic polynomial time algorithm which takes security parameter 1^λ as input and outputs a public-private key pair (PK, SK).
- **ENC(m, PK):** A probabilistic polynomial time algorithm which takes a message m and public key PK as input and returns ciphertext $\mathcal{C}$.
- **DEC($\mathcal{C}, SK, PK$):** A deterministic polynomial time algorithm which takes ciphertext $\mathcal{C}$, secret key SK and public key PK as input and returns a message m if $\mathcal{C}$ is a valid ciphertext else $\perp$.

Definition: Encryption Scheme

- **KG(1^λ):** A probabilistic polynomial time algorithm which takes security parameter 1^λ as input and outputs a public-private key pair (PK, SK).
- **ENC(m, PK):** A probabilistic polynomial time algorithm which takes a message m and public key PK as input and returns ciphertext $\mathcal{C}$.
- **DEC($\mathcal{C}, SK, PK$):** A deterministic polynomial time algorithm which takes ciphertext $\mathcal{C}$, secret key SK and public key PK as input and returns a message m if $\mathcal{C}$ is a valid ciphertext else $\perp$.

For consistency, it is required that for all $(PK, SK) \leftarrow \mathrm{KG}(1^\lambda)$ and all messages m, $m = \mathrm{DEC}(\mathrm{ENC}(m, PK), SK, PK)$.

Definition: IND-CPA

An encryption scheme S_{ENC} is said to be **IND-CPA (indistinguishable against chosen plaintext attack)** secure if no probabilistic polynomial time algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ has a non-negligible advantage in the following game:

Definition: IND-CPA

An encryption scheme S_{ENC} is said to be **IND-CPA (indistinguishable against chosen plaintext attack)** secure if no probabilistic polynomial time algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ has a non-negligible advantage in the following game:

$\underline{\textbf{Game}^{IND-CPA}_{S_{ENC},\mathcal{A}}}$

- $(PK, SK) \leftarrow \mathrm{KG}(1^\lambda)$
- $(m_0, m_1, st) \leftarrow \mathcal{A}_1(PK)$
- $b \xleftarrow{R} \{0, 1\}$
- $y \leftarrow ENC(m_b, PK)$
- $b' \leftarrow \mathcal{A}_2(y, PK, st)$

The advantage of $\mathcal{A}$ is defined as $\mathcal{A}dv(\mathcal{A}) = |\Pr(b = b') - \frac{1}{2}|$

Definition: IND-CCA

An encryption scheme S_{ENC} is said to be **IND-CCA (indistinguishable against chosen ciphertext attack)** secure if no probabilistic polynomial time algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ has a non-negligible advantage in the following game:

Definition: IND-CCA

An encryption scheme S_{ENC} is said to be **IND-CCA (indistinguishable against chosen ciphertext attack)** secure if no probabilistic polynomial time algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ has a non-negligible advantage in the following game:

- *DecryptionOracle*$(\mathcal{O})$: Given a ciphertext $\mathcal{C}$, except the challenge ciphertext, the oracle returns $m \leftarrow \mathrm{DEC}(\mathcal{C}, SK, PK)$.

Game$^{IND-CCA}_{S_{ENC},\mathcal{A}}$

- $(PK, SK) \leftarrow \mathrm{KG}(1^\lambda)$
- $(m_0, m_1, st) \leftarrow \mathcal{A}_1^{\mathcal{O}}(PK)$
- $b \xleftarrow{R} \{0, 1\}$
- $y \leftarrow \mathrm{ENC}(m_b, PK)$
- $b' \leftarrow \mathcal{A}_2^{\mathcal{O}}(y, PK, st)$

The advantage of $\mathcal{A}$ is defined as $\mathcal{A}dv(\mathcal{A}) = |\Pr(b = b') - \frac{1}{2}|$

Definition: IND-CCVA

An encryption scheme S_{ENC} is said to be **IND-CCVA (indistinguishable against chosen ciphertext verification attack)** secure if no probabilistic polynomial time algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ has a non-negligible advantage in the following game:

Definition: IND-CCVA

An encryption scheme S_{ENC} is said to be **IND-CCVA (indistinguishable against chosen ciphertext verification attack)** secure if no probabilistic polynomial time algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ has a non-negligible advantage in the following game:

- *ChosenCiphertextVerificationOracle*$(\mathcal{O})$: Given a ciphertext $\mathcal{C}$, the oracle returns 1 if $\mathcal{C}$ is valid else returns 0.

Game$^{IND-CCVA}_{S_{ENC},\mathcal{A}}$

- $(PK, SK) \leftarrow \mathrm{KG}(1^\lambda)$
- $(m_0, m_1, st) \leftarrow \mathcal{A}_1^{\mathcal{O}}(PK)$
- $b \xleftarrow{R} \{0,1\}$
- $y \leftarrow \mathrm{ENC}(m_b, PK)$
- $b' \leftarrow \mathcal{A}_2^{\mathcal{O}}(y, PK, st)$

The advantage of $\mathcal{A}$ is defined as $\mathcal{A}dv(\mathcal{A}) = \left|\Pr(b = b') - \frac{1}{2}\right|$

Trivial Conclusions

1. IND-CCVA secure encryption schemes are IND-CPA secure also.
   IND-CCVA $\rightarrow$ IND-CPA
2. IND-CCA secure encryption schemes are IND-CCVA secure also.
   IND-CCA $\rightarrow$ IND-CCVA

Does CCVA make sense?

PKCS#1

- **KG(1^λ):** Choose primes p, q ($4k$ bit each) and compute $n = pq$ (n is k byte number). Choose e, d, such that $ed \equiv 1 \pmod{\phi(n)}$. The public key, PK, is (n, e) and the secret key, SK, is (p, q, d).
- **ENC(m, PK):** A data block D, consisting of $|D|$ bytes, is encrypted as follows:
  - First, a padding string PS, consisting of $k - 3 - |D|$ nonzero bytes, is generated pseudo-randomly (the byte length of PS is atleast 8).
  - Now, the encryption block $EB = 00||02||PS||00||D$ is formed, is converted into an integer x, and is encrypted with RSA, giving the ciphertext $c = x^e \pmod{n}$.

- **DEC(c, SK, PK)** A Ciphertext c is decrypted as follows:
  - Compute $x' = c^d \pmod{n}$.
  - Converts x' into an encryption block EB'.
  - Check, if the encryption block is PKCS *conforming* (An encryption block EB consisting of k bytes, $EB = EB_1||\ldots||EB_k$, is called PKCS conforming, if it satisfies the following conditions: $EB_1 = 00$, $EB_2 = 02$, EB_3 through EB_{10} are nonzero and at least one of the bytes EB_{11} through EB_k is 00).
  - If the encryption block is PKCS conforming, then output the data block; otherwise an error sign.

Bleichenbacher's Attack on PKCS#1

Bleichenbacher's attack assumes that the adversary has access to an oracle that, for every ciphertext, returns whether the corresponding plaintext is PKCS conforming. If the plaintext is not PKCS conforming, the oracle outputs an error sign. Given just these error signs, because of specific properties of PKCS #1, Bleichenbacher showed how a very clever program can decrypt a target ciphertext (the oracle answer will reveal the first two bytes of the corresponding plaintext of the chosen ciphertext).

Bleichenbacher's Attack on PKCS#1

Bleichenbacher's attack assumes that the adversary has access to an oracle that, for every ciphertext, returns whether the corresponding plaintext is PKCS conforming. If the plaintext is not PKCS conforming, the oracle outputs an error sign. Given just these error signs, because of specific properties of PKCS #1, Bleichenbacher showed how a very clever program can decrypt a target ciphertext (the oracle answer will reveal the first two bytes of the corresponding plaintext of the chosen ciphertext).

D. Bleichenbacher. *Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1.* In Proc. Crypto'98, pages 1-12, 1998.

- CCVA makes sense.

- CCVA makes sense.

Questions

1. Does there exist any encryption scheme which is IND-CCVA secure but not IND-CCA secure?
2. Does there exist any encryption scheme which is IND-CPA secure but not IND-CCVA secure?

Generic Constructions

IND-CCVA secure but not IND-CCA secure

Let $\prod$ be a public key encryption scheme with $\mathcal{K}$ as key space, $\mathcal{M}$ as message space, and $\mathcal{C}$ as ciphertext space. In general, we have

$$\cup_{k\in\mathcal{K}}\mathsf{Enc}(\mathcal{M}) \subseteq \mathcal{C}.$$

IND-CCVA secure but not IND-CCA secure

Let $\prod$ be a public key encryption scheme with $\mathcal{K}$ as key space, $\mathcal{M}$ as message space, and $\mathcal{C}$ as ciphertext space. In general, we have

$$\cup_{k\in\mathcal{K}}\mathsf{Enc}(\mathcal{M}) \subseteq \mathcal{C}.$$

If

- $\prod$ is IND-CPA secure but not IND-CCA secure, and
- $\cup_{k\in\mathcal{K}}\mathsf{Enc}(\mathcal{M}) = \mathcal{C}$

IND-CCVA secure but not IND-CCA secure

Let $\prod$ be a public key encryption scheme with $\mathcal{K}$ as key space, $\mathcal{M}$ as message space, and $\mathcal{C}$ as ciphertext space. In general, we have

$$\cup_{k \in \mathcal{K}} \mathsf{Enc}(\mathcal{M}) \subseteq \mathcal{C}.$$

If

- $\prod$ is IND-CPA secure but not IND-CCA secure, and
- $\cup_{k \in \mathcal{K}} \mathsf{Enc}(\mathcal{M}) = \mathcal{C}$

then,

- There exists an IND-CCVA secure encryption scheme but not IND-CCA secure.

IND-CCVA secure but not IND-CCA secure (2)

Let

- $\prod$ is IND-CPA secure but not IND-CCA secure, and
- $\cup_{k \in \mathcal{K}} \mathsf{Enc}(\mathcal{M}) = \mathcal{C}$

IND-CCVA secure but not IND-CCA secure (2)

Let

- $\prod$ is IND-CPA secure but not IND-CCA secure, and
- $\cup_{k \in \mathcal{K}} \mathsf{Enc}(\mathcal{M}) = \mathcal{C}$

$\hat{\mathcal{E}} = (KeyGen_{\hat{\mathcal{E}}}, ENC_{\hat{\mathcal{E}}}, DEC_{\hat{\mathcal{E}}})$ based on $\prod$

- $KeyGen_{\hat{\mathcal{E}}}$: Same as $KeyGen$.
- $ENC_{\hat{\mathcal{E}}}$: Encryption of a message m under a public key PK is given as
$$\hat{c} = 1||c, \text{ where } c = ENC(m, PK).$$
- $DEC_{\hat{\mathcal{E}}}$:
$$DEC_{\hat{\mathcal{E}}}(\hat{c}, SK, PK) = DEC(c, SK, PK) \text{ if } \hat{c} = 1||c, \text{ otherwise return } \perp.$$

IND-CCVA secure but not IND-CCA secure (2)

Let

- $\prod$ is IND-CPA secure but not IND-CCA secure, and
- $\cup_{k \in \mathcal{K}} \mathsf{Enc}(\mathcal{M}) = \mathcal{C}$

$\hat{\mathcal{E}} = (KeyGen_{\hat{\mathcal{E}}}, ENC_{\hat{\mathcal{E}}}, DEC_{\hat{\mathcal{E}}})$ based on $\prod$

- $KeyGen_{\hat{\mathcal{E}}}$: Same as $KeyGen$.
- $ENC_{\hat{\mathcal{E}}}$: Encryption of a message m under a public key PK is given as
$$\hat{c} = 1||c, \text{ where } c = ENC(m, PK).$$
- $DEC_{\hat{\mathcal{E}}}$:
$$DEC_{\hat{\mathcal{E}}}(\hat{c}, SK, PK) = DEC(c, SK, PK) \text{ if } \hat{c} = 1||c, \text{ otherwise return } \perp.$$
- $\hat{\mathcal{E}}$ is IND-CPA secure but not IND-CCA secure, and
- $\cup_{k \in \mathcal{K}} \mathsf{Enc}(\mathcal{M}) \neq \mathcal{C}$

It is easy to check that $\hat{\mathcal{E}}$ is IND-CPA secure but not IND-CCA secure with the added property that every ciphertext need not be valid. Since it is trivial to distinguish valid ciphertexts from invalid ciphertexts (by just looking at the most significant bit), CCVA oracle does not give any extra advantage to the adversary and thus $\hat{\mathcal{E}}$ is IND-CCVA secure.

IND-CPA secure but not IND-CCVA secure

Let $\mathcal{E}_{CPA}$ be a public key encryption scheme described by the key generation algorithm $KeyGen_{CPA}$, encryption algorithm ENC_{CPA} and decryption algorithm DEC_{CPA}. Now define a new public key encryption $\mathcal{E}$ as follows

IND-CPA secure but not IND-CCVA secure

Let $\mathcal{E}_{CPA}$ be a public key encryption scheme described by the key generation algorithm $KeyGen_{CPA}$, encryption algorithm ENC_{CPA} and decryption algorithm DEC_{CPA}. Now define a new public key encryption $\mathcal{E}$ as follows

- KeyGen: Same as $KeyGen_{CPA}$.
- Enc: Encryption of a message m under a public key PK is given as

$$c = c_1||c_2 = ENC_{CPA}(m, PK)||ENC_{CPA}(m, PK)$$

- Dec: Decryption of a ciphertext $c = c_1||c_2$ with the corresponding secret key SK will proceed as follows:
    - $m_1' \leftarrow DEC_{CPA}(c_1, SK, PK)$
    - $m_2' \leftarrow DEC_{CPA}(c_2, SK, PK)$
    - If $m_1' = m_2'$, return m_1', else
    - return $\perp$

IND-CPA secure but not IND-CCVA secure

- Attack

$$b \xrightarrow{\mathcal{R}} \{0, 1\}$$
$$\mathcal{C}_b = c_1^b || c_2^b = ENC_{CPA}(m_b, PK) || ENC_{CPA}(m_b, PK)$$

IND-CPA secure but not IND-CCVA secure

- Attack

$$b \xrightarrow{\mathcal{R}} \{0,1\}$$
$$\mathcal{C}_b = c_1^b || c_2^b = ENC_{CPA}(m_b, PK) || ENC_{CPA}(m_b, PK)$$
$$\downarrow$$
$$b' \xrightarrow{\mathcal{R}} \{0,1\}$$
$$\mathcal{C}_{b'} = c_1^b || c_2^{b'} = ENC_{CPA}(m_b, PK) || ENC_{CPA}(m_{b'}, PK)$$

- Attack

$$b \xrightarrow{\mathcal{R}} \{0, 1\}$$
$$\mathcal{C}_b = c_1^b || c_2^b = ENC_{CPA}(m_b, PK) || ENC_{CPA}(m_b, PK)$$
$$\downarrow$$
$$b' \xrightarrow{\mathcal{R}} \{0, 1\}$$
$$\mathcal{C}_{b'} = c_1^b || c_2^{b'} = ENC_{CPA}(m_b, PK) || ENC_{CPA}(m_{b'}, PK)$$
$$\downarrow$$

if chosen ciphertext verification oracle returns 1, $b = b'$, else $b \neq b'$

IND-CCA1 secure but not IND-CCVA secure

Let $\mathcal{E}_{CCA1}$ be a public key encryption scheme described by the key generation algorithm $KeyGen_{CCA1}$, encryption algorithm ENC_{CCA1} and decryption algorithm DEC_{CCA1}. Now define a new public key encryption $\mathcal{E}$ as follows

- KeyGen: Same as $KeyGen_{CCA1}$.
- Enc: Encryption of a message m under a public key PK is given as

$$c = c_1 || c_2 = ENC_{CCA1}(m, PK) || ENC_{CCA1}(m, PK)$$

- Dec: Decryption of a ciphertext $c = c_1||c_2$ with the corresponding secret key SK will proceed as follows:
  - $m'_1 \leftarrow DEC_{CCA1}(c_1, SK, PK)$
  - $m'_2 \leftarrow DEC_{CCA1}(c_2, SK, PK)$
  - If $m'_1 = m'_2$, return m'_1, else
  - return $\perp$

IND-CCA1 secure but not IND-CCVA secure

- Attack

$$b \xrightarrow{\mathcal{R}} \{0, 1\}$$
$$\mathcal{C}_b = c_1^b || c_2^b = ENC_{CCA1}(m_b, PK) || ENC_{CCA1}(m_b, PK)$$

IND-CCA1 secure but not IND-CCVA secure

- Attack

$$b \xrightarrow{\mathcal{R}} \{0,1\}$$
$$\mathcal{C}_b = c_1^b || c_2^b = ENC_{CCA1}(m_b, PK) || ENC_{CCA1}(m_b, PK)$$
$$\downarrow$$
$$b' \xrightarrow{\mathcal{R}} \{0,1\}$$
$$\mathcal{C}_{b'} = c_1^b || c_2^{b'} = ENC_{CCA1}(m_b, PK) || ENC_{CCA1}(m_{b'}, PK)$$

IND-CCA1 secure but not IND-CCVA secure

- Attack

$$b \xrightarrow{\mathcal{R}} \{0,1\}$$
$$\mathcal{C}_b = c_1^b || c_2^b = ENC_{CCA1}(m_b, PK) || ENC_{CCA1}(m_b, PK)$$
$$\downarrow$$
$$b' \xrightarrow{\mathcal{R}} \{0,1\}$$
$$\mathcal{C}_{b'} = c_1^b || c_2^{b'} = ENC_{CCA1}(m_b, PK) || ENC_{CCA1}(m_{b'}, PK)$$
$$\downarrow$$

if chosen ciphertext verification oracle returns 1, $b = b'$, else $b \neq b'$

- There exists an IND-CCA1 secure encryption scheme but not IND-CCVA secure.

Thank You