VERSITA

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/tmmp-2013-0039
Tatra Mt. Math. Publ. **57** (2013), 119–121

A NOTE ON "ON CIPHERTEXT UNDETECTABILITY"

Angsuman Das — Avishek Adhikari

ABSTRACT. The notion of ciphertext undetectability was introduced in [Gaži, P. – Stanek, M.: *On ciphertext undetectability*, Tatra Mt. Math. Publ. **41** (2008), 133–151] as a steganographic property of an encryption scheme. While finding the relationship between ciphertext undetectability and indistinguishability of encryptions, authors showed that ciphertext undetectability does not imply indistinguishability. Though the proposition is correct, the proof is not. In this note, we provide a correct proof of the above-mentioned result by a slight modification of the construction used in original paper cited above.

1. Introduction

In [1], authors introduced the novel notion of ciphertext undetectability (CUD) as a steganographic property of a public-key encryption scheme (PKE). Informally, an encryption scheme has the property of ciphertext undetectability, if the attacker is unable to distinguish between valid and invalid ciphertexts. Moreover, the inter-relationships between ciphertext undetectability and other existing well-studied security notions are discussed in [1].

In Theorem 4.2 of Section 4.1 [1], authors showed that there exists PKEs which are CUD-secure but not IND-CPA secure. However, we point out a flaw in the proof and propose a modified construction to prove the same result. For notations and preliminaries, see [1].

2. Definition of ciphertext undetectability

Let $S = (G, E, D)$ be a public key encryption with ciphertext space $\overline{\mathcal{C}}$. Also, let us denote by $\mathcal{C}_v$, the set of all valid ciphertexts, i.e., $\mathcal{C}_v = \left\{c \in \overline{\mathcal{C}} : D(c) \neq \perp\right\}$. Formally, an adversary A, running in two phases *ask* and *guess*, for attacking ciphertext undetectability behaves as follows.

2010 Mathematics Subject Classification: 94A60, 68P25.
Keywords: security notions, ciphertext undetectability, indistinguishability of encryption.

In the first stage of the adversary's attack, A takes a public key pk, and outputs some state information s. The challenger chooses $b \in \{0,1\}$ randomly. If $b = 1$, challenger chooses $c^* \in_R \mathcal{C}_v$, else chooses $c^* \in_R \overline{\mathcal{C}} \setminus \mathcal{C}_v$. In the guess phase, A guesses b' for the hidden bit b.

- **Set up:** The challenger picks $(pk, sk) \leftarrow G(1^k)$ and gives pk to A.
- **Query Phase I:** A is given access to the oracle $D_1(\cdot)$.
- **Challenge Phase:** The challenger flips a random coin $b \leftarrow \{0,1\}$ and receives some state information s from A. If $b = 0$, challenger chooses $c^* \in \mathcal{C}_v$ randomly, else choose $c^* \in_R \overline{\mathcal{C}} \setminus \mathcal{C}_v$, and gives c^* and s to A.
- **Query Phase II:** A is given access to the oracle $D_2(\cdot)$.
- **Output Phase:** A outputs a bit b'. The *advantage of* A in this game is given by $\mathsf{Adv}^{cud-atk}_{S,\overline{\mathcal{C}},A}(k) = 2Pr[b' = b] - 1$.

Finally, an encryption scheme $S = (G, E, D)$ is said to be CUD $-atk$ secure, $atk \in \{\text{CPA,CCA1,CCA2}\}$ if

1. $\mathcal{C}_v \subsetneq \overline{\mathcal{C}}$,
2. there exists a deterministic polynomial algorithm, which accepts exactly the set $\overline{\mathcal{C}}$,
3. $\mathsf{Adv}^{cud-atk}_{S,\overline{\mathcal{C}},A}(k)$ is negligible, where A ranges through all polynomial time probabilistic adversaries.

2.1. Construction used in Theorem 4.2 of [1]

Let $atk \in \{\text{CPA,CCA1,CCA2}\}$ be an attack model. Let $S = (G, E, D)$ be a CUD-atk secure scheme with plaintext space $\mathcal{P}$. Consider the scheme $S' = (G', E', D)$:

$G'(1^k)$	$E'_{pk'}(m)$
$G(1^k) \to (pk, sk)$	If $m = m^+$
$m^+ \in_R \mathcal{P};\ c^+ := E_{pk}(m^+)$	return c^+
Set $pk' = (pk, m^+, c^+), sk' = sk$	Else, return $E_{pk}(m)$
return (pk', sk')	

FIGURE 1. Construction used in Theorem 4.2 of [1].

In the proof of the Theorem 4.2 in [1], authors claimed that S' is also CUD $-atk$ secure as the sets of valid ciphertexts of S and S' are same. However, that is not true. Consider the set of all possible ciphertexts of m^+ in S, apart from c^+. This subset consists of valid ciphertexts if considered w.r.t S, however they are invalid if considered w.r.t S'. The reason is that only c^+ can be the valid ciphertext corresponding to m^+ in S'. This creates the difference in the set of valid ciphertexts of S and S'. We fix this flaw by suitably modifying their construction in the following section.

3. Modified construction and proof

Theorem 3.1 (CUD-$atk \not\Rightarrow$ IND-CPA). *If there exists an encryption scheme* Π *which is secure in the sense of* CUD $-atk$*, then there exists another encryption scheme which is secure in the sense of* CUD $-atk$*, but not secure in* IND-CPA *sense, for any attack* $atk \in \{\text{CPA}, \text{CCA1}, \text{CCA2}\}$.

Proof. Let $S = (G, E, D)$ be an CUD $-atk$ secure public key encryption scheme with plaintext space $\mathcal{P}$. Consider a new scheme $S' = (G', E', D)$, where G', E' are modified as in Fig. 2 and D is kept unaltered.

$G'(1^k)$	$E'_{pk'}(m)$
$G(1^k) \to (pk, sk)$	If $m = m^+$
$m^+ \in_R \mathcal{P};\ c^+ := E(m^+)$	$\beta \in_R \{0,1\}^k$
$pk' = (pk, m^+, c^+)$	If $\beta = 0^k$, return $E(m)$
$sk' = sk$	else, return c^+
return (pk', sk')	Else, return $E(m)$

Figure 2. Modified construction.

Clearly, the above construction in Fig. 2 is not IND-CPA secure as the encryption of a publicly known message m^+ is almost deterministic, i.e, it returns c^+ with an overwhelming probability of $1 - \frac{1}{2^k}$. On the other hand, the construction also ensures that the set of valid ciphertexts are same for both S and S'. By a simple reduction it can be shown that S' is CUD-atk secure if S is so. □

REFERENCES

[1] GAŽI, P.—STANEK, M.: *On Ciphertext Undetectability*, Tatra Mt. Math. Publ. **41** (2008), 133–151, eprint.iacr.org/2007/388.pdf.

Received December 30, 2013

Angsuman Das
Department of Mathematics
St. Xavier's College
Kolkata
INDIA
E-mail: angsumandas054@gmail.com

Avishek Adhikari
Department of Pure Mathematics
University of Calcutta
Kolkata
INDIA
E-mail: avishek.adh@gmail.com