On the Impossibility of Strong Encryption over $\aleph_0$

Raphael C.-W. Phan[1⋆] and Serge Vaudenay[2]

[1] Loughborough Uni, U.K.
[2] EPFL, Switzerland

Abstract. We give two impossibility results regarding strong encryption over an infinite enumerable domain. The first one relates to statistically secure one-time encryption. The second one relates to computationally secure encryption resisting adaptive chosen ciphertext attacks in streaming mode with bounded resources: memory, time delay or output length. Curiously, both impossibility results can be achieved with either finite or continuous domains. The latter result explains why known CCA-secure cryptosystem constructions require at least two passes to decrypt a message with bounded resources.

1 Introduction

As the cardinality of sets increases, it is a well known fact from set theory that some mathematical problems can suddenly become impossible to solve then become possible again. For instance, for any logical assertion on finite sets we can always decide whether it is true of false. When the set becomes infinite but enumerable (that is, the cardinality of $\aleph_0$ following the Cantor notion) some mathematical statements can become undecidable as shown by Gödel with the Peano arithmetic. That is, statements of the form

$$\forall x\ \exists y \quad f(x,y) = 0$$

may be undecidable even though f has a polynomial form with integral variables and coefficients. When sets become larger, e.g. the cardinality $2^{\aleph_0}$ of continuous sets, predicates based on inequalities can be decided. That is, over logical assertion with elementary formula of form $f(x) = 0$ or $f(x) > 0$ can be decided as shown by Tarski [29].

Assuming the continuum hypothesis we have $\aleph_1 = 2^{\aleph_0}$ but $\aleph_1$ can be smaller otherwise. This hypothesis is undecidable in the standard Zermelo-Fraenkel set theory axiomatic with the axiom of choice.

In cryptography, results on strong encryption are well understood. Since Shannon, we know how to achieve perfect secrecy on finite sets by using the Vernam cipher (aka one-time pad). One-time pad can also be defined on the continuous unit interval $[0,1]$ by using the modulo 1 addition of a message and a

⋆ Part of work done while the author was with EPFL, Switzerland.

key. However, it was shown by Chor and Kushilevitz [9, 10] that it was impossible to achieve over $\aleph_0$ under some ad-hoc generalization of the Shannon secrecy.

Similarly, we can construct computationally secure encryption (in the sense of security against chosen-ciphertext adversaries) using hybrid encryption [12]. However, all proposed constructions require scanning the ciphertext twice for decryption so the decryption algorithm cannot work with finite resources in streaming mode over $\aleph_0$. In practice, this necessarily wastes resources in time and in memory. An open problem [1, 2] is whether strong encryption schemes exist that can be streamlined, and more so the case when the domain is infinite.

In this paper, we first revisit the Chor-Kushilevitz result. We show that their notion of security is unnecessarily strong and show the impossibility over $\aleph_0$ with a weaker notion. We then analyze the practicality of strong encryption, i.e. if it is possible to achieve strong encryption when the scheme's resources are bounded, either in memory or in time. Indeed, when a provably secure scheme especially one for which has infinite domain is implemented in practice, bounded resources are an inevitable artifact. In this setting, one wonders if the provable security results are preserved from theory to practice. If security is preserved, this indicates that the strong encryption scheme even one with infinite domain can be streamlined since bounded resources imply that an infinite input cannot be processed immediately but necessarily requires streamlining.

To be precise, by bounded memory we mean that as the scheme's encryption or decryption process is streamlined, its internal state utilized during the process has a bound which is a polynomial function of the security parameter. By bounded time, we mean that the scheme's process issues the output stream only after some delay, rather than immediately as input streams are received. To this end, we can alternatively model the latter as the process issuing outputs of bounded length.

1.1 Related Work

In a different direction but related to the context of bounded resources, researchers have studied security models in which *adversaries* have bounded memory [26, 19], as a compromise to achieve information theoretic security against computationally unbounded adversaries.

The first known provable security notion for (public-key) encryption is indistinguishability (IND) (or so called polynomial security) [18], which has an equivalent alternative definition called semantic security [18]. These characterizations did not consider adversarial access to the decryption oracle, and thus fall within the chosen-plaintext adversarial model (CPA). Later IND characterizations refined this to the chosen-ciphertext adversarial model (CCA) [27, 28, 8].

Given that the CCA adversarial model allows the adversary access to the decryption oracle, the basic idea in the design of CCA-secure schemes is to make this decryption oracle useless to the adversary in terms of breaking IND. For this, some implicit or explicit form of validity check [25] is typically designed into the decryption algorithms of these schemes. This necessitates having two passes

over the text input: for encryption, the first pass over the plaintext to obtain the ciphertext while the second pass over the plaintext is to generate a validity-checking tag for later verification when decrypting ciphertext; for decryption, the first pass over the ciphertext decrypts it to obtain the plaintext and the second pass over the text verifies if it actually corresponds to the received tag before the plaintext is actually output.

While two passes currently seem inevitable for strong security, indeed no known strong encryption schemes exist with a single pass; yet for practical uses (e.g. these days it is common to be downloading hundreds of megabytes of data over the Internet) it is advantageous to achieve a streaming capability, i.e. the second pass can start before the end of the first pass; sort of similar to the concept of streaming video: start watching before the entire movie is downloaded. This has efficiency implications, e.g. there is no need to buffer the entire text, and the encryption/decryption speed increases. Achievement of streamability for strong encryption would indicate that strong encryption schemes over infinite domains exist.

For the symmetric (blockwise) encryption context, the concept of *online* encryption and decryption [3, 4, 13, 14] has been considered. The motivation for this is related to the desire to provide a kind of streaming capability without needing to buffer the entire text or wait until the entire text is received before it starts to be processed. To be precise, online means that the output block can be returned on the fly in one pass, given only the key, the current input block and previous input and output blocks: the rest of the input blocks are not required for returning the output block up to this point. IND notions have been proposed for this particular setting to consider blockwise-adaptive adversaries [21, 15], in both CPA and CCA style adversarial models [15, 14, 4].

It is known [9, 10] that weakly secure (in some statistical sense) symmetric encryption is impossible over infinite sets such as $\{0,1\}^*$ although it is possible over larger sets such as $[0,1]$. As for public-key encryption, statistical security is of course impossible so we have to consider computational security.

2 Preliminaries

Let $\mathcal{A}^*$ denote the set of finite sequences of elements in a set $\mathcal{A}$; ε denote a sequence of length zero so that $\varepsilon \in \mathcal{A}^*$ for any $\mathcal{A}$; $x \in_U \mathcal{A}$ denote uniformly selecting an element in a set $\mathcal{A}$; and $\|$ denote the concatenation operation in $\mathcal{A}^*$. For $x \in \mathcal{A}^*$, $|x|$ denotes the length of x; $\aleph_0$ denotes the cardinality of the set of natural numbers $\mathbb{N}$, which is the smallest possible infinite set.

In the sequel, we consider encryption over the infinite domain $\{0,1\}^*$. For technical reasons we formalize this domain by a prefix-free language $\mathcal{C} = \{0,1\}^*\|\top$, i.e. the set of words consisting of an arbitrary bitstring terminated by the special $\top$ symbol. When considering messages given as bit streams, this symbol indicates that the message is complete.

2.1 Public Key Encryption (PKE)

A public-key encryption scheme PKE consists of three algorithms, $\mathsf{PKE.KeyGen}$, $\mathsf{PKE.Enc}$, and $\mathsf{PKE.Dec}$. It must be such that there exists some integer κ for which:

1. $\langle pk, sk\rangle \leftarrow \mathsf{PKE.KeyGen}(1^\lambda)$: A probabilistic algorithm that on input the security parameter λ, generates public and private keys $\langle pk, sk\rangle$ by taking time bounded by λ^κ for some integer κ.
2. $c \leftarrow \mathsf{PKE.Enc}_{pk}(m; r)$: A probabilistic algorithm that encrypts a message $m \in \mathcal{M}$ into a ciphertext c by using some random coins r and taking time bounded by $(|m| + \lambda)^\kappa$.
3. $m \leftarrow \mathsf{PKE.Dec}_{sk}(c)$: An algorithm that decrypts c by taking time bounded by $(|c| + \lambda)^\kappa$. It outputs either $m \in \mathcal{M}$ or a special symbol $\perp \notin \mathcal{M}$. An obvious correctness condition applies.

Let A_E be a polynomial-time oracle machine that plays the following adaptive chosen-ciphertext game:

[IND-ATK PKE] Game
1: $\langle pk, sk\rangle \leftarrow \mathsf{PKE.KeyGen}(1^\lambda)$
2: $\langle m_0, m_1, \rho\rangle \leftarrow A_E^{\mathcal{O}_1^{\mathsf{ATK}}}(pk)$
3: $b \in_U \{0,1\}$; $r \in_U \{0,1\}^{(|m_0|+\lambda)^\kappa}$; $c^* \leftarrow \mathsf{PKE.Enc}_{pk}(m_b; r)$
4: $\tilde{b} \leftarrow A_E^{\mathcal{O}_2^{\mathsf{ATK}}}(\rho, c^*)$
Note that it is required for $|m_0| = |m_1|$.

Depending on how the decryption oracles $\mathcal{O}_1^{\mathsf{ATK}}$ and $\mathcal{O}_2^{\mathsf{ATK}}$ are defined, different characterizations of the game can be obtained to capture relevant security notions. For instance, to capture notions related to indistinguishability against adaptive chosen-ciphertext attacks ($\mathsf{IND\text{-}CCA}$) [28], $\mathcal{O}_1^{\mathsf{ATK}}$ is defined as:

Oracle $\mathcal{O}_1^{\mathsf{CCA}}(c)$
1: $m \leftarrow \mathsf{PKE.Dec}_{sk}(c)$
2: **return** m

Here, the oracle terminates and returns control to the adversary A_E via the **return** statement. Meanwhile it is required that A_E be restricted not to ask c^* to $\mathcal{O}_2^{\mathsf{ATK}}$, i.e. $\mathcal{O}_2^{\mathsf{ATK}}$ only replies to queries that do not equal the challenge ciphertext c^*:

Oracle $\mathcal{O}_2^{\mathsf{CCA}}(c)$
1: **if** $c \neq c^*$ **then**
2: $\quad m \leftarrow \mathsf{PKE.Dec}_{sk}(c)$
3: $\quad$ **return** m
4: **else**
5: $\quad$ **return** $\perp$
6: **end if**

This can be relaxed in an IND-rCCA game [8], where the decryption oracle $\mathcal{O}_2^{\mathsf{ATK}}$ behaves as follows:

Oracle $\mathcal{O}_2^{\mathsf{rCCA}}(c)$
1: $m \leftarrow \mathsf{PKE.Dec}_{sk}(c)$
2: **if** $m \notin \{m_0, m_1\}$ **then**
3: **return** m
4: **else**
5: **return** $\perp$
6: **end if**

In the much weaker IND-CPA game [18], the oracle $\mathcal{O}_2^{\mathsf{ATK}}$ is unavailable by definition:

Oracle $\mathcal{O}_2^{\mathsf{CPA}}(c)$
1: **return** $\perp$

Note that in the context of PKEs, the encryption oracle is public by construction. For symmetric encryption, however, access to the encryption oracle characterizes [22, 23] an additional dimension to the adversary's capability and hence corresponding security notion. In that case, an even weaker notion, so-called *one-time encryption* (IND-OTE) game [12, 24] and capturing passive security makes even the encryption oracle unavailable to the adversary.

We define $\mathbf{Adv}^{\mathsf{IND\text{-}ATK}}_{PKE,A_E} = |\Pr[\tilde{b} = b] - \frac{1}{2}|$ and

$$\mathbf{Adv}^{\mathsf{IND\text{-}ATK}}_{PKE} = \max_{A_E}(\mathbf{Adv}^{\mathsf{IND\text{-}ATK}}_{PKE,A_E})$$

where maximum is taken over all ppt machines. We say that a PKE is IND-ATK-secure if $\mathbf{Adv}^{\mathsf{IND\text{-}ATK}}_{PKE}$ is negligible in λ, where $\mathsf{ATK} \in \{\mathsf{CCA}, \mathsf{rCCA}, \mathsf{CPA}\}$.

2.2 Some Streamline Cryptosystems

As already observed, known IND-CCA-secure constructions require decryption to scan the ciphertext at least twice. However, encryption can process by scanning the plaintext once. Examples include the well-known Cramer-Shoup scheme [11] and variants [12], different forms of hybrid encryption [12, 2, 1, 20], and identity-based encryption (IBE) schemes [7, 5, 6, 25].

If we now relax the security notion down to IND-CPA security, we can achieve secure stream encryption with bounded resources. Consider a public-key encryption scheme OLDPKE over a finite domain (e.g., RSA). Consider a pseudorandom generator PRG whose input lies in the encryption domain. Namely, for any integer n, PRG_n is a function producing an n-bit string from some random coins. We define an encryption scheme NEWPKE by:

1. $\mathsf{NEWPKE.KeyGen} = \mathsf{OLDPKE.KeyGen}$
2. $\mathsf{NEWPKE.Enc}_{pk}(m; \langle k, r\rangle) = \langle \mathsf{OLDPKE.Enc}_{pk}(k; r), m \oplus \mathsf{PRG}_{|m|}(k)\rangle$
3. $\mathsf{NEWPKE.Dec}_{sk}(\langle c, c'\rangle) = c' \oplus \mathsf{PRG}_{|c'|}(\mathsf{OLDPKE.Dec}_{sk}(c))$

Clearly, both encryption and decryption can process streams with bounded resources.

Theorem 1. *If OLDPKE is* IND-CPA*-secure and PRG is* IND*-secure then NEW-PKE is* IND-CPA*-secure.*

We recall that IND security for PRG is defined by the following game:

[**IND PRG**] **Game**
1: $\langle 1^n, \rho\rangle \leftarrow A(1^\lambda)$
2: $b \in_U \{0,1\}$; $k \in_U \mathcal{K}$;
3: **if** $b = 0$ **then**
4: $\quad c \leftarrow \mathsf{PRG}_n(k)$
5: **else**
6: $\quad c \in_U \{0,1\}^n$
7: **end if**
8: $\tilde{b} \leftarrow A(\rho, c)$

Proof. Let Γ_1^b be the IND-CPA game conditioned to the value of bit b. Note that the 3rd step of Γ_1^b is

3: $k \in_U \mathcal{K}$; $r \in_U \{0,1\}^{(|m_0|+\lambda)^\kappa}$; $c_1^* \leftarrow \mathsf{OLDPKE.Enc}_{pk}(k; r)$;
$c_2^* \leftarrow m_b \oplus \mathsf{PRG}_{|m_b|}(k)$; $c^* = \langle c_1^*, c_2^*\rangle$

Given a ppt A_E and a game Γ, we denote by $\Gamma(A_E)$ the event that A_E wins. For instance, $\Gamma_1^b(A_E)$ is the event that A_E produces $\tilde{b}$ which equals b. We want to prove that for any A_E, $\Pr[\Gamma_1^0(A_E)] - \Pr[\Gamma_1^1(A_E)]$ is negligible.

Let Γ_2^b be the same game in which the 3rd step of Γ_1^b is replaced by

3: $k \in_U \mathcal{K}$; $k' \in_U \mathcal{K}$; $r \in_U \{0,1\}^{(|m_0|+\lambda)^\kappa}$; $r' \in_U \{0,1\}^{(|m_0|+\lambda)^\kappa}$;
$c_1^* \leftarrow \mathsf{OLDPKE.Enc}_{pk}(k'; r')$; $c_2^* \leftarrow m_b \oplus \mathsf{PRG}_{|m_b|}(k)$; $c^* = \langle c_1^*, c_2^*\rangle$

We construct A'_E an adversary playing the IND-CPA game for OLDPKE by using A_E playing either Γ_1^b or Γ_2^b as follows: the generation of r, r', and the computation of c_1^* are outsourced to the IND-CPA game and A'_E only submit the two plaintexts k and k'. A'_E produces $\tilde{b}$ as a final bit. We let $\Gamma^{b'}$ denote the IND-CPA game for OLDPKE with bit b'. Clearly, we have $\Pr[\Gamma_1^b(A_E)] = \Pr[\Gamma^0(A'_E)]$ and $\Pr[\Gamma_2^b(A_E)] = \Pr[\Gamma^1(A'_E)]$ since the winning condition is $\tilde{b} = b$ in all cases. As OLDPKE is IND-CPA-secure we obtain that $\Pr[\Gamma_1^b(A_E)] - \Pr[\Gamma_2^b(A_E)]$ is negligible.

Let now Γ_3^b be the Γ_2^b game in which the 3rd step is replaced by

3: $k \in_U \mathcal{K}$; $r \in_U \{0,1\}^{(|m_0|+\lambda)^\kappa}$; $\mathsf{random} \in_R \{0,1\}^{|m|}$;
$c_1^* \leftarrow \mathsf{OLDPKE.Enc}_{pk}(k; r)$; $c_2^* \leftarrow m_b \oplus \mathsf{random}$; $c^* = \langle c_1^*, c_2^*\rangle$

We construct A'' an adversary playing the IND game for PRG by using A_E playing either Γ_2^b or Γ_3^b as follows: the generation of k' and the computation of either $\mathsf{PRG}_{|m_b|}(k')$ or random are outsourced to the IND game. We let $\tilde{\Gamma}^{b''}$ denote the IND game for PRG with bit b''. Clearly, we have $\Pr[\Gamma_2^b(A_E)] = \Pr[\tilde{\Gamma}^0(A'')]$ and

$\Pr[\Gamma_3^b(A_E)] = \Pr[\tilde{\Gamma}^1(A'')]$. Since PRG is IND-secure we obtain that $\Pr[\Gamma_2^b(A_E)] - \Pr[\Gamma_3^b(A_E)]$ is negligible.

Let now Γ_4^b be the Γ_3^b game in which the 3rd step is replaced by

3: $k \in_U \mathcal{K}$; $r \in_U \{0,1\}^{(|m_0|+\lambda)^\kappa}$; $\mathsf{random} \in_R \{0,1\}^{|m|}$;
$c_1^* \leftarrow \mathsf{OLDPKE.Enc}_{pk}(k; r)$; $c_2^* \leftarrow \mathsf{random}$; $c^* = \langle c_1^*, c_2^* \rangle$

Clearly, Γ_3^b and Γ_4^b produce c^* of same distribution so $\Pr[\Gamma_3^b(A_E)] = \Pr[\Gamma_4^b(A_E)]$.

To summarize, we have that $\Pr[\Gamma_1^b(A_E)] - \Pr[\Gamma_4^b(A_E)]$ is negligible. Since we trivially have $\Pr[\Gamma_4^0(A_E)] = \Pr[\Gamma_4^1(A_E)]$ we obtain that $\Pr[\Gamma_1^0(A_E)] - \Pr[\Gamma_1^1(A_E)]$ is negligible. □

3 Statistically-Secure Encryption

Throughout this section, we assume that all sets are enumerable so that we deal with discrete probability theory.

Given two distributions P_0 and P_1 for a random variable X the statistical distance is

$$d(P_0, P_1) = \frac{1}{2} \sum_x \left| \Pr_{P_0}[X = x] - \Pr_{P_1}[X = x] \right|$$

The statistical distance is the exact measure to characterize the advantage of the best distinguisher between the two distributions when using a single sample. When the statistical distance is negligible, the distributions are statistically indistinguishable.

A *cipher* is defined by a distribution for a secret key K and a function Enc mapping (x, k) to $\mathsf{Enc}_k(x) = y$ such that Enc_k is collision-free, so that we can invert it. Given a random plaintext X which is independent from K, we define the random ciphertext $Y = \mathsf{Enc}_K(X)$. We say that a security notion relative to a cipher is *universal* if it does not depend on the distribution of X.

Shannon's notion of perfect secrecy is defined by the statistical independence of X and Y. Although this definition does not look like universal at a first glance, we can easily see that it is equivalent to the property that the function $(x, y) \mapsto \Pr[\mathsf{Enc}_K(x) = y]$ only depends on y. This is a universal notion since it only depends on the cipher design and not on the distribution of X.

Given a possible ciphertext y, the *a posteriori distribution* P_y of X given y is the marginal distribution of X conditioned to $Y = y$. Let P be the a priori distribution of X. We have

$$\begin{aligned} d(P, P_y) &= \frac{1}{2} \sum_x |\Pr[X = x] - \Pr[X = x | Y = y]| \\ &= \frac{1}{2} \sum_x \Pr[X = x] \left| 1 - \frac{\Pr[\mathsf{Enc}_K(x) = y]}{\Pr[Y = y]} \right| \end{aligned}$$

Shannon's secrecy can be defined by saying that $d(P, P_y) = 0$ for all y that can occur. The next question relates to how to relax this security definition so that secrecy is no longer perfect but is still universal and achieves some kind of statistical security. A natural extension would we the following one.

Definition 2. *A cipher provides ε-imperfect secrecy if for any distribution of X and all possible y we have $d(P, P_y) \leq \varepsilon$.*

In [9, 10], Chor and Kushilevitz propose the following definition.

Definition 3. *Given $\alpha \geq 1$, a cipher provides α-weak secrecy if for all $x_1, x_2 \in \mathsf{Supp}(X)$ and all y we have*

$$\frac{1}{\alpha} \Pr[Y = y | X = x_2] \leq \Pr[Y = y | X = x_1] \leq \alpha \Pr[Y = y | X = x_2]$$

where $\mathsf{Supp}(X)$ is the set of all possible values of X. This property is universal.

Clearly, 1-weak secrecy is equivalent to Shannon's perfect secrecy. If the cipher achieves α-weak secrecy, for any x and any possible y, the ratio between $\Pr[Y = y|X = x]$ and $\Pr[Y = y]$ is between $\frac{1}{\alpha}$ and α, so we have $d(P, P_y) \leq \frac{\alpha-1}{2}$. We deduce the following theorem.

Theorem 4. *α-weak secrecy implies $\frac{\alpha-1}{2}$-imperfect secrecy.*

One drawback of α-weak secrecy is expressed by the following result.

Theorem 5 (Chor-Kushilevitz [9, 10]). *If a cipher provides α-weak secrecy then its domain must be finite.*

Proof. Assuming that a cipher provides α-weak secrecy, we can take a possible plaintext x_2 and a possible key k. We let $y = \mathsf{Enc}_k(x_2)$ so $\Pr[Y = y|X = x_2] \neq 0$. We have that for all x_1 in $\mathsf{Supp}(X)$,

$$\Pr[Y = y | X = x_1] \geq \frac{1}{\alpha} \Pr[Y = y | X = x_2] > 0$$

but the left-hand side is just $\Pr[\mathsf{Dec}_K(y) = x_1]$ so summing over many x_1's should be at most 1. We deduce that the plaintext domain must be finite. □

We can now consider the notion of indistinguishability between the encryption of two arbitrary plaintexts. That is, given a plaintext x we consider the distribution Q_x for $\mathsf{Enc}_K(x)$.

Definition 6. *A cipher is ε-statistically indistinguishable under one-time encryption (IND-OTE) if for all x_1 and x_2 we have $d(Q_{x_1}, Q_{x_2}) \leq \varepsilon$.*

Clearly, this notion is universal. We have

$$d(Q_{x_1}, Q_{x_2}) = \frac{1}{2} \sum_y |\Pr[Y = y | X = x_1] - \Pr[Y = y | X = x_2]|$$

Clearly, if we have α-weak secrecy, we have $d(Q_{x_1}, Q_{x_2}) \leq \frac{\alpha-1}{2}$. We deduce the following theorem.

Theorem 7. *α-weak secrecy implies $\frac{\alpha-1}{2}$-statistically IND-OTE.*

The converse is not true as the following example shows.

Example 8. Let $\{0,1\}$ be the plaintext domain. Let $k = (\kappa, \beta)$ be composed by an integer κ and a bit β such that $\Pr[K = k] = \frac{1}{2}2^{-\kappa-1}$. We define

$$\mathsf{Enc}_k(b) = \begin{cases} \kappa \| (\beta \oplus b) & \text{if } \kappa < n \\ (\kappa \| \beta) + 2b & \text{otherwise} \end{cases}$$

Given a ciphertext $y = z\|t$ with $t \in \{0,1\}$, we have $\Pr[\mathsf{Enc}_K(0) = y] = \frac{1}{2}2^{-z-1}$ and

$$\Pr[\mathsf{Enc}_K(1) = y] = \begin{cases} \Pr[\mathsf{Enc}_K(0) = y] & \text{if } z < n \\ 0 & \text{if } z = n \\ 2\Pr[\mathsf{Enc}_K(0) = y] & \text{if } z > n \end{cases}$$

thus the cipher does not provide α-weak secrecy for any $\alpha < 2$. Assuming an a priori distribution of the plaintext we notice that $\Pr[X = 1 | Y = n\|t] = 0$ whereas $\Pr[X = 0 | Y = n\|t] = \frac{1}{2}$. So, we have $d(P, P_{n\|t}) = \frac{1}{4}$. The cipher does not provide ε-imperfect secrecy for any $\varepsilon < \frac{1}{4}$. However,

$$d(Q_0, Q_1) = \sum_{t=0}^{1} \left(\sum_{z=n}^{+\infty} \Pr[\mathsf{Enc}_K(0) = n\|t] \right) = \sum_{z=n}^{+\infty} 2^{-z-1} = 2^{-n}$$

so the cipher is 2^{-n}-IND-OTE secure.

The above example shows that α-weak secrecy is sufficient for IND-OTE security but not necessary. Furthermore, the natural extension of Shannon's perfect secrecy by the notion of imperfect secrecy appears insufficient to capture the notion of statistical security. So, the feasibility of IND-OTE secure encryption over an infinite domain is a legitimate question. We answer below by the negative.

Theorem 9. *Let $\varepsilon < 1$. If a given cipher is ε-statistically* IND-OTE *secure then its plaintext domain is finite.*

Proof. Let x_1 be an arbitrary reference plaintext in the domain. We have that $\sum_y \Pr[\mathsf{Enc}_K(x_1) = y] = 1$ so there must exist a finite set A such that the sum for $y \in A$ is greater than $\frac{1+\varepsilon}{2}$. For any x_2 in the domain we have

$$\begin{aligned} \sum_{y \in A} \Pr[\mathsf{Enc}_K(x_2) = y] &= \sum_{y \in A} \Pr[\mathsf{Enc}_K(x_1) = y] - \\ &\quad \sum_{y \in A} (\Pr[\mathsf{Enc}_K(x_1) = y] - \Pr[\mathsf{Enc}_K(x_2) = y]) \\ &\geq \frac{1+\varepsilon}{2} - \varepsilon \\ &= \frac{1-\varepsilon}{2} \end{aligned}$$

Since

$$\begin{aligned} \sum_{x_2 \in \mathsf{Domain}} \sum_{y \in A} \Pr[\mathsf{Enc}_K(x_2) = y] &= \sum_{y \in A} \sum_{x_2 \in \mathsf{Domain}} \Pr[\mathsf{Dec}_K(y) = x_2] \\ &\leq \#A \end{aligned}$$

we obtain that $\#A \geq \frac{1-\varepsilon}{2}\#\mathsf{Domain}$ so the domain is finite. □

4 Strong Encryption over $\aleph_0$ with Bounded Memory

Definition 10. *Let $\mathcal{Z}$ be an alphabet. A **streamline** function with state space $\mathcal{S}$ over $\mathcal{Z}$ is a family $F = (f_c)_{c\in\mathcal{Z}}$ of functions:*

$$f_c : \mathcal{S} \to \mathcal{Z}^* \times \mathcal{S}.$$

By abuse of notation, we define

$$f_c(y, s) = \langle y \| y', s' \rangle$$

where $\langle y', s' \rangle = f_c(s)$. We also define

$$f_x(y, s) = (f_{x_m} \circ \cdots \circ f_{x_1})(y, s)$$

where $x = x_1 \cdots x_m$. Given $x \in \mathcal{Z}^*$ and $s \in \mathcal{S}$, we further define the function $F_s : \mathcal{Z}^* \to \mathcal{Z}^*$ by $f_x(\varepsilon, s) = \langle F_s(x), \cdot \rangle$.

A function over a language is called **monotonic** if for any x and y in the language, the image of x is a prefix of the image of y whenever x is a prefix of y. Note that all functions defined over a prefix code $\mathcal{C}$ are monotonic.

The following fact is pretty trivial:

Lemma 11. *For a streamline function F with state space $\mathcal{S}$ over $\mathcal{Z}$ and $s \in \mathcal{S}$, the function F_s is monotonic.*

Definition 12. *A monotonic function $G : \mathcal{C} \to \mathcal{Z}^*$ over a subset $\mathcal{C}$ of $\mathcal{Z}^*$ is **streamlineable with σ states** if there exists a streamline function F with a state space $\mathcal{S}$ of σ elements and $s \in \mathcal{S}$ such that G equals F_s restricted to $\mathcal{C}$. We call F_s an **implementation** of G with σ states.*

Lemma 13. *All monotonic functions $G : \mathcal{C} \to \mathcal{Z}^*$ on a subset $\mathcal{C}$ of $\mathcal{Z}^*$ are streamlineable with $\aleph_0$ states.*

The idea is to store the input of G in a state and to output something as soon as possible.

Proof. We define $\bar{G} : \mathcal{Z}^* \to \mathcal{Z}^*$ by $\bar{G}(x) = G(y)$ where y is the longest prefix of x in $\mathcal{C}$ if any and $\bar{G}(x) = \varepsilon$ otherwise. Clearly, $\bar{G}$ is monotonic and equal to G when restricted to $\mathcal{C}$. Let $\mathcal{S} = \mathcal{Z}^*$ and define

$$f_c(s) = \langle \mathsf{drop}_{\bar{G}(s)} \bar{G}(s\|c), s\|c \rangle,$$

where $\mathsf{drop}_y(x)$ denotes string x with prefix y dropped (e.g. if $x = y\|z$, then $\mathsf{drop}_y(x) = z$). We easily show that F_ε is an implementation of G for $F = (f_c)_{c\in\mathcal{Z}}$. □

Theorem 14. *Let us consider an* IND-rCCA*-secure public-key encryption scheme over $\mathcal{M} = \{0,1\}^*\|\top$. For any key pair, the decryption function is not streamlineable with a finite number of states.*

Proof. Let $\mathcal{Z} = \{0, 1, \top, \bot\}$ and $\mathcal{M} = \{0,1\}^* \| \top$. Here $\top$ is a special character which indicates a word termination so that $\mathcal{M}$ is a prefix code. We consider a PKE over $\mathcal{M}$. Given a key pair, encryption resp. decryption can be defined by a function $\bar{G}_r$ resp. D verifying:

1. $\bar{G}_r : \mathcal{C} \to \mathcal{C}$ is an injective function for any random coins r and
2. $D : \mathcal{C} \to \mathcal{C} \cup \{\bot\}$ is a function such that $D \circ \bar{G}_r(x) = x$ for any $x \in \mathcal{C}$ and any r.

We assume that D is streamlineable with σ states and later show that the PKE is not IND-rCCA-secure.

Let $s \in \mathcal{S}$, and $G = (g_c)_{c \in \mathcal{Z}}$ be such that $|\mathcal{S}| = \sigma$, G_s is an implementation of D with σ states, where g_c corresponding to G_s is as in Definition 10.

Let $\mathsf{bit}_\ell(x)$ denotes the ℓth character of x. Clearly, for $x \in \mathcal{M}$ we have

$$x = \mathsf{trunc}_{|x|-2}(x) \| \mathsf{bit}_{|x|-1}(x) \| \top.$$

Let $\mathcal{C}_k = \{0,1\}^k \| \top$. Let r be fixed. Given x, let ℓ_x be the minimal integer such that $D(\mathsf{trunc}_{\ell_x}(\bar{G}_r(x)) \| \top) = x$. Clearly, $1 \leq \ell_x \leq |\bar{G}_r(x)| - 1$. We define

$$Z(x) = g_{\mathsf{trunc}_{\ell_x - 1}(\bar{G}_r(x))}(\varepsilon, s).$$

For some probabilistic encryption $\bar{G}_r(x)$, we interpret $Z(x)$ to be the pair with a partial decryption of $\bar{G}_r(x)$ together with the internal state of the decryption algorithm D. By definition, we have:

$$\langle x, \cdot \rangle = g_\top \circ g_{\mathsf{bit}_{\ell_x}(\bar{G}_r(x))}(Z(x))$$

and

$$\mathsf{bit}_{\ell_x}(\bar{G}_r(x)) \in \{0, 1\}.$$

Let $\mathcal{X} = \{x \in \mathcal{C}_k : Z(x) \in \{\varepsilon\} \times \mathcal{S}\}$. This is the set of plaintexts x of length k such that the partial decryption of $\bar{G}_r(x)$ is empty. We have

$$\sigma \geq |Z(\mathcal{X})| \geq \frac{|\mathcal{X}|}{2}.$$

Hence

$$\Pr_{x \in_U \mathcal{C}_k}[Z(x) \in \{\varepsilon\} \times \mathcal{S}] \leq \frac{2\sigma}{2^k}.$$

If $x \notin \mathcal{X}$ we let $Z(x) = \langle y, s' \rangle$. Since $y \neq \varepsilon$, we have that y is a prefix of $G_s(\mathsf{trunc}_{\ell_x}(\bar{G}_r(x)) \| z)$ for any z. For z such that $\mathsf{trunc}_{\ell_x}(\bar{G}_r(x)) \| z = \bar{G}_r(x)$ we obtain that y is a prefix of x. For $z = \top$, we obtain that y is also a prefix of $D(\mathsf{trunc}_{\ell_x - 1}(\bar{G}_r(x)) \| \top)$. Hence, $D(\mathsf{trunc}_{\ell_x - 1}(\bar{G}_r(x)) \| \top) \notin \{\bot, x\}$ and it returns a string whose first bit is $\mathsf{trunc}_1(x)$.

Let T denote the event that

$$\mathsf{trunc}_1(D(\mathsf{trunc}_{\ell_x - 1}(\bar{G}_r(x)) \| \top)) = \mathsf{trunc}_1(x).$$

Therefore

$$\Pr_{x \in_U \mathcal{C}_k}[T] \geq 1 - \frac{2\sigma}{2^k}.$$

This holds for any implementation of D with σ states, and for any r so it holds for random choices of r as well. For $k \geq \log_2 \sigma + 3$, we have

$$\Pr[T] \geq \frac{3}{4}. \tag{1}$$

Let A_E be defined as follows:

$A_E^{\mathcal{O}_1^{\mathsf{rCCA}}}(pk)$
1: pick m_0 and m_1 of length $k = \lceil \log_2 \sigma + 3 \rceil$ with different first bit at random
2: **return** m_0, m_1, and $\rho = \mathsf{trunc}_1(m_0)$

$A_E^{\mathcal{O}_2^{\mathsf{rCCA}}}(\rho, c^*)$
1: $\ell \leftarrow |c^*|$
2: **repeat**
3: $\quad \ell \leftarrow \ell - 1$
4: $\quad \tilde{m} \leftarrow \mathcal{O}_2^{\mathsf{rCCA}}(\mathsf{trunc}_{\ell-1}(c^*) \| \top)$
5: **until** $\tilde{m} \neq \perp$ or $\ell = 1$
6: **if** $\mathsf{trunc}_1(\tilde{m}) \in \{0, 1\}$ **then**
7: $\quad$ **return** $\mathsf{trunc}_1(\tilde{m}) \oplus \rho$
8: **else**
9: $\quad$ **return** a random bit
10: **end if**

Clearly, while $\ell > \ell_{m_b}$ the rCCA oracle answers $\perp$ because the decryption leads to m_b. When $\ell = \ell_{m_b}$, the decryption is different from m_b so the rCCA oracle is not censored. Then T holds with probability at least $\frac{3}{4}$. In this case, the oracle returns a string whose first bit is the one of m_b Hence, if T occurs as soon as $\ell = \ell_{m_b}$, we must have $b = \tilde{b}$. We obtain the advantage of A_E to win the game as

$$\begin{aligned}
\mathbf{Adv}^{\mathsf{IND\text{-}rCCA}}_{PKE, A_E} &\geq \Pr[\tilde{b} = b] - \frac{1}{2} \\
&\geq \Pr[T] - \frac{1}{2} \\
&\geq \frac{1}{4}.
\end{aligned}$$

Thus with non-negligible advantage an adversary A_E will win the IND-rCCA PKE game; and so a PKE with infinite domain and streamlineable decryption with σ states cannot achieve IND-rCCA security when σ is polynomially bounded. □

This result is further supported by the fact that definitions of the decryption algorithm for all known IND-CCA PKE schemes over infinite domains require two passes: one for decrypting the ciphertext and one for validity check of the decryption result.

In essence, this answers the question about the (in)existence of strong encryption schemes with streaming capability. We have shown that IND-rCCA-secure encryption schemes with streaming encryption exist, but the decryption cannot be streamlined.

Clearly, the same result applies to IND-rCCA-secure symmetric encryption.

5 Strong Encryption over $\aleph_0$ with Bounded Time

We consider here a more general definition of functions on streams with bounded resources. Instead of imposing a finite memory (or equivalently a finite number of states) we require that for each new symbol the number of output symbols is bounded; that is, in other words, the delay for returning something given an input stream is bounded.

Definition 15. *Let $\mathcal{Z}$ be an alphabet, and Δ be some non-negative integer. A streamline function $F = (f_c)_{c\in\mathcal{Z}}$ is called Δ-**delayed** if for any s we have*

$$|(f_c(s))_1| \leq \Delta.$$

Clearly, given a streamline function F over a state space $\mathcal{S}$, if $\mathcal{Z}$ and $\mathcal{S}$ are finite, there exists Δ such that F is Δ-delayed.

Theorem 16. *Let us consider an* IND-rCCA*-secure public-key encryption scheme over $\mathcal{M} = \{0,1\}^*\top$. For any key pair and any Δ, the decryption function is not Δ-delayed.*

Proof. With the same notations as in the proof of Theorem 14, for $k > 2\Delta$ we have

$$g_{\mathsf{trunc}_{\ell_x-1}(\bar{G}_r(x))}(\varepsilon, x) \notin \{\varepsilon\} \times \mathcal{S}$$

since $g_{\mathsf{trunc}_{\ell_x-1}(\bar{G}_r(x))}$ and $g_\top$ have outputs limited to length Δ each and $D(\bar{G}_r(x)) = x$ of length $|x| = k$. Hence, T occurs with probability 1 and our IND-rCCA adversary has advantage at least $\frac{1}{2}$. □

6 Secure Encryption over a Continuous Domain

The previous results show the infeasibility of weakly secure encryption over the infinite but enumerable $\aleph_0$ domain. As the domain grows up we have to deal with non-enumerable sets (e.g. the set of real numbers of cardinality $2^{\aleph_0}$) so we have to revisit all definitions for this latter case.

The standard Shannon notion of perfect secrecy adapts well by the notion of statistical independence of X and Y for any distribution of X. We first show

that perfect secrecy can be achieved over the continuous set of cardinality $2^{\aleph_0}$ taken from the unit interval $[0,1]$. We take a uniformly distributed key K in $[0,1]$ and define $\mathsf{Enc}_k(x) = (x+k) \bmod 1$.

For any density probability function f for X and for any measurable sets A and B of $[0,1]$ we have that

$$\Pr[X \in A, Y \in B] = \int_{x \in A} f(x) \Pr[x + K \in B]\, dx$$

since $\Pr[x+K \in B] = \mu(B)$ is not dependent on x we obtain $\Pr[X \in A, Y \in B] = \Pr[X \in A]\mu(B)$. Applying this equation for $A = [0,1]$ we obtain $\Pr[Y \in B] = \mu(B)$ thus for all A and B we have $\Pr[X \in A, Y \in B] = \Pr[X \in A] \Pr[Y \in B]$: X and Y are statistically independent for any distribution of X. Thus, the cipher provides perfect secrecy.

The question of computational security for this case is a little harder since the computational model is not adapted to operations with real numbers.

To define a computational model able to deal with $2^{\aleph_0}$ we should be able to handle algorithms taking infinite sequences of bits as input and returning another infinite sequence of bits. More precisely, an infinite sequence $s = \{s_i\}_{i=0}^{n}$ of bits is an encoding of a real number from the interval $[0,1]$. (To avoid confusion we refer to s as a *real number* instead of a sequence.) This implies having memory units able to store such reals and elementary operations on this type of data.

More precisely, given an algorithm $\mathcal{A}$ mapping m bits $a_1, \ldots, a_m$ to n bits $b_1, \ldots, b_n$ in t steps the new Turing machine shall be able to map m reals $\alpha_1, \ldots, \alpha_m$ into n reals $\beta_1, \ldots, \beta_n$ in such a way that the ith bits of the β's are obtained by using $\mathcal{A}$ applied to the ith bits of the α's. We obtain a kind of "free" parallelism this way.

We shall also use arithmetic operations on real numbers in $[0,1]$ as well as simple bit manipulations in the sequence. Assuming a prefix-free encoding of an arbitrary bitstring, an infinite sequence of bits can be interpreted as a sequence of bitstrings. Therefore we can use operations over sequence of bits to define operations over sequences of bitstrings. We can do this to extend the operations on bitstrings to operations on sequences of bitstrings by using the free parallelism. For instance, we can concatenate two sequence of bitstrings coordinate-wise. We can extract the sequence of the ith bit of a sequence of bitstrings, etc.

The notion of stream of reals which cannot be stored with constant memory becomes irrelevant since a list of reals can be encoded into a single sequence of bits: a list of reals can be compressed into a single real. Clearly, the problem of handling stream of reals with constant time and memory boils down to the problem of encrypting a single real number.

Assuming that IND-CPA secure public key encryption over the domain $\{0,1\}$ is feasible with these kinds of devices, we can transform it into an IND-CCA secure cryptosystem over the set of reals by adapting the Fujisaki-Okamoto transform [16, 17] in the random oracle model.

In more detail, given an IND-CPA secure public key encryption OLDPKE over the bit domain $\{0,1\}$, we can define an IND-CPA secure public key encryption TMPPKE over reals where the encryption algorithm $\mathsf{TMPPKE.Enc}_{pk}(m;r)$ takes as input a (potentially infinite) sequence $m = \{m_i\}_{i=0}^{n}$ of bits m_i and a sequence $r = \{r_i\}_{i=0}^{n}$ of random strings r_i; more precisely we have:

1. $\mathsf{TMPPKE.KeyGen} = \mathsf{OLDPKE.KeyGen}$
2. $\mathsf{TMPPKE.Enc}_{pk}(m;r) = \{\mathsf{OLDPKE.Enc}_{pk}(m_i;r_i)\}_{i=0}^{n}$
3. $\mathsf{TMPPKE.Dec}_{sk}(c) = \{\mathsf{OLDPKE.Dec}_{sk}(c_i)\}_{i=0}^{n}$

Next, we construct an IND-CCA secure public key encryption NEWPKE as:

1. $\mathsf{NEWPKE.KeyGen} = \mathsf{TMPPKE.KeyGen}$
2. $\mathsf{NEWPKE.Enc}_{pk}(m;r) = \mathsf{TMPPKE.Enc}_{pk}(\langle m,r\rangle; H(\langle m,r\rangle))$
3. $\mathsf{NEWPKE.Dec}_{sk}(c) =$
   (a) $\langle m',h'\rangle = \mathsf{TMPPKE.Dec}_{sk}(c)$
   (b) **if** $c = \mathsf{TMPPKE.Enc}_{pk}(m';h')$, **return** m'

where $\langle a,b\rangle$ denotes the concatenation of the prefix-free encoding of a and b applied in parallel on all coordinates; and $H(x)$ denotes a random oracle call used to compute a sequence of bitstrings of appropriate length.

We could investigate further and consider constructions without random oracles, but this would be beyond our purpose. Our point is that secure and efficient encryption over a domain larger than $\aleph_0$ is feasible (modulo the required adaptations of the computational model).

7 Conclusion

We studied the imperfect notion of secrecy for one-time encryption. We proved that the one by Chor and Kushilevitz is too strong to capture statistical indistinguishability. We extended their impossibility result for encryption over $\aleph_0$ to a weaker notion.

We have shown the decryption (of bitstrings) cannot be implemented in streaming mode with bounded resources without losing the security against adaptive chosen-ciphertext attacks. These results explain the reason why existing CCA-secure encryption schemes are designed with decryption that necessarily performs two passes over the ciphertext before a plaintext is output; and indicate the inexistence of strong encryption schemes over infinite domains. The practical implications of this is that one needs to make a decision tradeoff: between strong encryption (if streamlineability is not required) versus efficiency in practice i.e. streaming capability (if strong encryption is not absolutely mandatory).

We finally observed that those impossibility results are contradicted when the domain is larger, e.g. with $2^{\aleph_0}$. This kind of paradoxical situation reminds some classical results from logic about decidability which can be lost over infinite domains and recovered over yet larger ones.

References

1. M. Abe, R. Gennaro, K. Kurosawa and V. Shoup, "Tag-KEM/DEM: A New Framework for Hybrid Encryption and a New Analysis of Kurosawa-Desmedt KEM," *Advances in Cryptology – EUROCRYPT '05*, LNCS 3494, pp. 128–146, Springer-Verlag, 2005.
2. M. Abe, R. Gennaro and K. Kurosawa, "Tag-KEM/DEM: A New Framework for Hybrid Encryption," *Journal of Cryptology*, Vol. 21, No. 1, pp. 97–130, 2008. Available at IACR ePrint Archive, `http://eprint.iacr.org/2005/027`.
3. M. Bellare, A. Boldyreva, L. Knudsen and C. Namprempre, "On-line Ciphers and the Hash-CBC Constructios," *Advances in Cryptology – CRYPTO '01*, LNCS 2139, pp. 292–309, Springer-Verlag, 2001. Full version available at `http://www-cse.ucsd.edu/users/mihir/papers/olc.html`.
4. A. Boldyreva and N. Taesombut, "On-line Encryption Schemes: New Security Notions and Constructions," *Topics in Cryptology – CT-RSA '04*, LNCS 2964, pp. 1–14, Springer-Verlag, 2004.
5. D. Boneh and J. Katz, "Improved Efficiency for CCA-Secure Cryptosystems Built using Identity-based Encryption," *Topics in Cryptology – CT-RSA '05*, LNCS 3376, pp. 87–103, Springer-Verlag, 2005.
6. D. Boneh, R. Canetti, S. Halevi and J. Katz, "Chosen-Ciphertext Security from Identity-based Encryption," *SIAM Journal of Computing*, Vol. 36, No. 5, pp. 1301–1328, 2007.
7. R. Canetti, S. Halevi and J. Katz, "Chosen-ciphertext Security from Identity-based Encryption," *Advances in Cryptology – EUROCRYPT '04*, LNCS 3027, pp. 207–222, Springer-Verlag, 2004.
8. R. Canetti, H. Krawczyk and J.B. Nielsen, "Relaxing Chosen-Ciphertext Security," *Advances in Cryptology – CRYPTO '03*, LNCS 2729, pp. 565–582, Springer-Verlag, 2003. Full version available at IACR ePrint Archive, `http://eprint.iacr.org/2003/174`.
9. B. Chor and E. Kushilevitz, "Secret Sharing over Infinite Domains (Extended Abstract)," *Advances in Cryptology – CRYPTO '89*, LNCS 435, pp. 299–306, Springer-Verlag, 1990.
10. B. Chor and E. Kushilevitz, "Secret Sharing over Infinite Domains," *Journal of Cryptology*, Vol. 6, No. 2, pp. 87–95, 1993.
11. R. Cramer and V. Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack," *Advances in Cryptology – CRYPTO '98*, LNCS 1462, pp. 13–25, Springer-Verlag, 1998.
12. R. Cramer and V. Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack," *SIAM Journal of Computing*, Vol. 33, No. 1, pp. 167–226, 2004.
13. P.-A. Fouque, A. Joux, G. Martinet and F. Valette, "Authenticated On-line Encryption," *Proceedings of SAC '03*, LNCS 3006, pp. 145–159, Springer-Verlag, 2003.
14. P.-A. Fouque, A. Joux, and G. Poupard, "Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes," *Proceedings of SAC '04*, LNCS 3357, pp. 212–226, Springer-Verlag, 2004.
15. P.-A. Fouque, G. Martinet and G. Poupard, "Practical Symmetric On-line Encryption," *Proceedings of FSE '03*, LNCS 2887, pp. 362–375, Springer-Verlag, 2003.
16. E. Fujisaki and T. Okamoto, "How to Enhance the Security of Public-Key Encryption at Minimum Cost," *Proceedings of PKC '99*, LNCS 1560, pp. 53–68, Springer-Verlag, 1999.

17. E. Fujisaki and T. Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes," *Advances in Cryptology - Crypto '99*, LNCS 1666, pp. 537–554, Springer-Verlag, 1999.
18. S. Goldwasser and S. Micali, "Probabilistic Encryption," *Journal of Computer and System Sciences*, Vol. 28, pp. 270–299, 1984.
19. D. Harnik and M. Naor, "On Everlasting Security in the Hybrid Bounded Storage Model," *Proceedings of ICALP '06*, LNCS 4052, pp. 192–203, Springer-Verlag, 2006.
20. D. Hofheinz and E. Kiltz, "Secure Hybrid Encryption from Weakened Key Encapsulation," *Advances in Cryptology – CRYPTO '07*, LNCS 4622, pp. 553–571, Springer-Verlag, 2007.
21. A. Joux, G. Martinet and F. Valette, "Blockwise-Adaptive Attackers - Revisiting the (In)Security of Some Provably Secure Encryption Modes: CBC, GEM, IACBC," *Advances in Cryptology - CRYPTO '02*, LNCS 2442, pp. 17–30, Springer-Verlag, 2002.
22. J. Katz and M. Yung, "Complete Characterization of Security Notions for Probabilistic Private-Key Encryption," *Proceedings of ACM Syposium on the Theory of Computing (STOC '00)*, pp. 245–254, ACM Press, 2000.
23. J. Katz and M. Yung, "Complete Characterization of Security Notions for Probabilistic Private-Key Encryption," *Journal of Cryptology*, Vol. 19, No. 1, pp. 67–95, 2006.
24. E. Kiltz and J. Malone-Lee, "A General Construction of IND-CCA2 Secure Public Key Encryption," *IMA Cryptography and Coding '03*, LNCS 2898, pp. 152–166, Springer-Verlag, 2003.
25. E. Kiltz and Y. Vahlis, "CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption," *Topics in Cryptology – CT-RSA '08*, LNCS 4964, pp. 221–238, Springer-Verlag, 2008.
26. U. Maurer, "Conditionally-Perfect Secrecy and a Provably-Secure Randomized Cipher," *Journal of Cryptology*, Vol. 5, No. 1, pp. 53–66, 1992.
27. M. Naor and M. Yung, "Public-key Cryptosystems Provably Secure against Chosen Ciphertext Attacks," *Proceedings of ACM Syposium on the Theory of Computing (STOC '90)*, pp. 427–437, ACM Press, 1990.
28. C. Rackoff and D. Simon, "Non-interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack," *Advances in Cryptology – CRYPTO '91*, LNCS 576, pp. 433–444, Springer-Verlag, 1991.
29. A. Tarski. "A Decision Method for Elementary Algebra and Geometry," University of California Press, Berkeley, CA, 1951.