# Two New Efficient CCA-Secure Online Ciphers: MHCBC and MCBC *

Mridul Nandi
National Institute of Standards and Technology
mridul.nandi@gmail.com

September 20, 2008

**Abstract**

Online ciphers are those ciphers whose ciphertexts can be computed in real time by using a length-preserving encryption algorithm. HCBC1 and HCBC2 are two known examples of Hash Cipher Block Chaining online ciphers. The first construction is secure against chosen plaintext adversary (or called CPA-secure) whereas the latter is secure against chosen ciphertext adversary (or called CCA-secure). In this paper, we have provided simple security analysis of these online ciphers. We have also proposed two new more efficient chosen ciphertext secure online ciphers modified-HCBC (MHCBC) and modified-CBC (MCBC). If one uses a finite field multiplication based universal hash function, the former needs one less key and one less field multiplication compared to HCBC2. The MCBC does not need any universal hash function and it needs only one blockcipher key unlike the other three online ciphers where two independent keys (hash function and blockcipher) are required.

**Keywords**: online cipher, CBC, universal hash function, random permutation.

## 1 Introduction

In this paper we fix a finite group $(G, +)$ (e.g., $\{0,1\}^n$ with bitwise addition $\oplus$ for some fixed positive integer $n$). An element of $G$ is called a block. A cipher over a domain $D \subseteq G^+ := \cup_{i\geq 1} G^i$ is a keyed function family $\{F_K\}_{K\in\mathcal{K}}$, where $\mathcal{K}$ is a key space and for each key $K$, $F_K : D \to D$ is a length-preserving permutation on $D$ (i.e., for each $x \in D \cap G^i$, $F_K(x) \in G^i$). Any cipher over domain $G$ is called a blockcipher. An important blockcipher is AES [6] with domain $G = \{0,1\}^{128}$. The pseudorandom permutation or PRP and strong pseudorandom permutation [10] or SPRP are two well known security notions for ciphers. They are also called chosen plaintext secure or CPA-secure and chosen ciphertext secure or CCA-secure. Intuitively, a cipher is called PRP (or SPRP) if it is indistinguishable from the ideal cipher based on encryption queries (or both encryption and decryption queries respectively). Intuitively an ideal cipher on $D$ is chosen at random from $\mathsf{Perm}(D)$, the set of all permutations on $D$. If $D$ is an infinite set then we define the ideal cipher runtime as queries being asked to it. A similar definition can be found for an ideal online cipher as defined in figure 1. In this paper we are interested in online cipher with domain $G^+$ whose $i^{\text{th}}$ ciphertext block $C[i]$ is computable from the first $i$ plaintext blocks $M[1], \cdots, M[i]$. The computation of the $i^{\text{th}}$ ciphertext is determined by a function called block function. The above property is popularly called online property. One can show that online ciphers can not be PRP since the online property itself can be used to distinguish it from an ideal cipher. The appropriate security notions are CPA-online secure and CCA-online secure [1]. Informally an online cipher is CPA-online secure (or CCA-online secure) if it is indistinguishable from an

*A preliminary version of this paper appears in Advances in Cryptology - INDOCRYPT 2008, Lecture Notes in Computer Science Vol. ???, pp. ???, Springer-Verlag, 2008. This is the full version.

ideal online cipher (see figure 1) based on only encryption queries (or encryption and decryption queries both respectively). The possible candidates of online ciphers are in [3, 5, 8], most of which are different variants of Cipher Block Chaining modes or CBC. If $e \in \mathsf{Perm}(D)$ then the CBC based on $e$ with an initial value IV is defined as $e^{+}(x_1, \cdots, x_m) = (y_1, \cdots, y_m)$ where $y_i = E_K(y_{i-1} + x_i)$, $1 \leq i \leq m$ and $y_0 = \mathrm{IV}$. One can see that CBC based on any blockcipher is an online cipher. In [1] authors have shown that CBC with public or secret IV [3] and ABC [8] ciphers (another example of online cipher) are not CPA-secure online ciphers. In the same paper [1] a CPA-secure HCBC1 online cipher and CCA-secure HCBC2 online cipher have been proposed. These online ciphers need two keys, one is for blockcipher and other is for *Almost XOR Universal Hash family* or AXU-hash family [15], a special case of $\Delta$universal hash family [9, 14, 16].

**Applicability of online ciphers.** The known online ciphers Hash-CBC namely, HCBC1, HCBC2 and our constructions need current and previous plaintext block and previous cipher block to compute the current cipher block. Thus, online cipher could be used where encryption is made in an online manner with a very small amount of memory or buffer. It could be useful in scenarios where there is a constraint requiring length-preserving ciphertext. For example, one can think some ciphers dealing with fixed packet formats, legacy code and disk-sector encryption. In this situation, a length preserving PRP or SPRP can be used but potentially these may be costlier than online ciphers as these are stronger security notions than a CPA or CCA online secure.

| Name of Online cipher | CPA-secure | CCA-secure | # field multiplication | # BC | Key-size |
|---|---|---|---|---|---|
| HCBC1 [2] | ✓ | × | $m$ | $m$ | $n + k_{\mathrm{BC}}$ |
| HCBC2 [2] | ✓ | ✓ | $2m$ | $m$ | $2n + k_{\mathrm{BC}}$ |
| MHCBC | ✓ | ✓ | $m$ | $m$ | $n + k_{\mathrm{BC}}$ |
| MCBC | ✓ | ✓ | 0 | $2m + 1$ | $k_{\mathrm{BC}}$ |

Table 1: In this comparison universal hash function is based on the field multiplication as given in example 2.1. Here, $G = \{0,1\}^n$, the set of blocks and $k_{\mathrm{BC}}$ denotes the key size of the blockcipher. The number of multiplications and block-cipher (BC) invocations are given to encrypt a plaintext with $m$ blocks.

**Our contributions.** In this paper we have provided simple as well as concrete security analysis of HCBC1 and HCBC2. The proof idea can also be used in other online ciphers. For example, we have used the same approach to have security proof of our new proposals MHCBC and MCBC. These two new online ciphers have many advantages over the previous ciphers. MHCBC needs a universal hash function from $G$ to $G$ whereas HCBC2 needs a universal hash function from $G^2$ to $G$, which makes it a potential efficient candidate. For example, if we use field multiplication based universal hash function then we need one less field multiplication and one less key (see example 2.1). Our second construction modified-CBC or MCBC does not need any universal hash function. It needs only one blockcipher key. One can definitely replace the universal hash function of MHCBC by a blockcipher (since an ideal blockcipher is $\Delta$universal hash function, see example 2.2) at the cost of an extra new independent blockcipher key which eventually causes an extra key-scheduling algorithm. In this paper we have shown that if we use same blockcipher key then MHCBC is not CCA-secure. Thus, the security of MCBC indeed is not straightforward from that of MHCBC. Table 1 provides a comparison of these four online ciphers.

## 2 Basic Definition and Results

We write $M = (M[1], \cdots, M[m])$ where $M[i] \in G$ is the $i^{\mathrm{th}}$ block of $M$. For $1 \leq i \leq j \leq m$, $M[i..j]$ represents $(M[i], M[i+1], \cdots, M[j])$. If $j < i$ then by convention $M[i..j] = \lambda$, the empty string. $X \overset{*}{\leftarrow} S$ means that the random variable $X$ is chosen uniformly from a finite set $S$ and it is independent with all previously defined random variables. An equivalent phrase "at random" is also widely used in cryptology. Let $F : \mathcal{K} \times D \rightarrow R$ where $\mathcal{K}$ is a finite set. By abuse of notation we denote $\mathsf{f} \overset{*}{\leftarrow} F$ to mean that $\mathsf{f} := F_K$

where $K \xleftarrow{*} \mathcal{K}$. The interpolation probability of $F$ for any fixed tuple $\tau := ((M_1, C_1), \cdots, (M_q, C_q))$ is the probability $\Pr[\mathsf{f}(M_1) = C_1, \cdots, \mathsf{f}(M_q) = C_q]$. We define the set of all non-empty prefixes of $M_1, \cdots, M_q \in G^+$ as

$$\mathbb{P}_M = \mathbb{P}(M_1, \cdots, M_q) := \{N \in G^+ : N \prec M_i \text{ for some } i \leq q\}.$$

We denote $\sigma := \sigma(M_1, \cdots, M_q) = |\mathbb{P}(M_1, \cdots, M_q)|$. Clearly, $\sigma \leq \sum_{i=1}^{q} \|M_i\|$. For $p \in G^+$ with $\|p\| = m$, we define $\text{chop}(p) = p[1..m-1]$ and $\text{last}(p) = p[m]$. In other words, $p = (\text{chop}(p), \text{last}(p))$ where $\text{last}(p) \in G$ and $\text{chop}(p) \in G^*$. Note that if $p \in G$ then $\text{chop}(p) = \lambda$ and $\text{last}(p) = p$. By our convention, $\text{last}(\lambda) = \mathbf{0}$. Now we define $\mathbb{P}'_M = \mathbb{P}'(M_1, \cdots, M_q) := \{p' \in G^* : p' = \text{chop}(p) \text{ for some } p \in \mathbb{P}_M\}$. Let $\mathbf{P}(N, k) := N(N-1)\cdots(N-k+1)$ for any positive integer $k < N$. A function $H : \mathcal{K} \times D \to G$ is called $\varepsilon$-$\Delta$universal hash function with domain $D$ and key-space $\mathcal{K}$ if $\Pr[\mathsf{h}(x_1) = \mathsf{h}(x_2) + y] \leq \varepsilon, \forall x_1 \neq x_2 \in D, y \in G$ where $\mathsf{h}$ denotes $H(K, \cdot)$ and $K$ is chosen uniformly from $\mathcal{K}$. Now we state a simple and useful property of $\varepsilon$-$\Delta$universal hash function and provide two examples of universal hash function. An *uniform random permutation* or URP over $G$ is a random variable $E^u \xleftarrow{*} \mathsf{Perm}(G)$ (it means that $E^u$ is chosen uniformly and independently from $\mathsf{Perm}(G)$). It is an ideal candidate of a blockcipher.

**Lemma 2.1** *Let $H$ be an $\varepsilon$-$\Delta$universal hash function and let $(x_1, y_1), \cdots, (x_\sigma, y_\sigma) \in D \times G$ be distinct. Then,* $\Pr[\mathsf{h}(x_i) + y_i = \mathsf{h}(x_j) + y_j,\ 1 \leq i \neq j \leq \sigma] \leq \frac{\varepsilon\sigma(\sigma-1)}{2}$.

**Proof.** We prove that for any pair $(i, j)$ with $1 \leq i < j \leq \sigma$, $\Pr[\mathsf{h}(x_i) + y_i = \mathsf{h}(x_j) + y_j] \leq \varepsilon$. The rest is clear by summing over all possible pairs $(i, j)$.

**Case** $x_i \neq x_j$ **:** From the definition of $\Delta$universal hash function $\Pr[\mathsf{h}(x_i) = \mathsf{h}(x_j) + (y_j - y_i)] \leq \varepsilon$.
**Case** $x_i = x_j$ **:** Since $(x_i, y_i) \neq (x_j, y_j)$ we have $y_i \neq y_j$ and hence $\Pr[\mathsf{h}(x_i) + y_i = \mathsf{h}(x_j) + y_j] = 0$. ■

**Example 2.1** *Suppose $(G, +, \cdot)$ is a finite field. Let $D = G = \mathcal{K}$ then $H(K, x) = K \cdot x$ is $\frac{1}{N}$-$\Delta$universal hash function. This is true since the number of $K$'s such that $K \cdot (x_1 - x_2) = y$ is at most one. Similarly $D = G^2 = \mathcal{K}$. Let $H((K_1, K_2), (x, y)) = K_1 \cdot x + K_2 \cdot y$ then it is a $\frac{1}{N}$-$\Delta$universal hash function.*

**Example 2.2** *Let $E^u \xleftarrow{*} \mathsf{Perm}(G)$ then for any $x_1 \neq x_2 \in G$ and $y \in G \setminus \{\mathbf{0}\}$ we have* $\Pr[E^u(x_1) = E^u(x_2) + y] = \frac{1}{N-1}$. *If $y = \mathbf{0}$ then* $\Pr[E^u(x_1) = E^u(x_2) + y] = \Pr[E^u(x_1) = E^u(x_2)] = 0$. *Hence $E^u$ is $\frac{1}{N-1}$-$\Delta$universal hash function.*

By using a simple counting argument we can show that for any distinct $x_1, \cdots, x_k \in G$ and distinct $y_1, \cdots, y_k \in G$

$$\Pr[E^u(x_1) = y_1, \cdots, E^u(x_k) = y_k] = \frac{1}{\mathbf{P}(N, k)} \tag{1}$$

Since the number of permutations $\pi \in \mathsf{Perm}(G)$ such that $\pi(x_1) = y_1, \cdots, \pi(x_k) = y_k$ is $(N-k)!$ and $|\mathsf{Perm}(G)| = N!$. The above may not be true if $x_i$'s and $y_i$'s are random variables but we have similar result when these are independent with the uniform random permutation $E^u$.

**Proposition 2.2** *Let $X_1, Y_1, \cdots, X_k, Y_k$ be random variables taking values on $G$ and $E^u \xleftarrow{*} \mathsf{Perm}(G)$. Let $\mathsf{COLL}_{\text{in}}$ denote the event that $X_i$'s are not distinct, $\mathsf{COLL}_{\text{out}}$ denote the event that $Y_i$'s are not distinct then*

$$\Pr[E^u(X_1) = Y_1, \cdots, E^u(X_k) = Y_k] \geq \frac{1 - \Pr[\mathsf{COLL}_{\text{in}}] - \Pr[\mathsf{COLL}_{\text{out}}]}{\mathbf{P}(N, k)}. \tag{2}$$

**Proof.** We have $\Pr[\mathsf{COLL}] \leq \Pr[\mathsf{COLL}_{\text{in}}] + \Pr[\mathsf{COLL}_{\text{out}}]$. Let $D = \{\mathbf{a} = (a_1, \cdots, a_k) \in G^k : a_i\text{'s are distinct}\}$ then $\mathsf{DIST}$ is true if and only if $(X_1, \cdots, X_k), (Y_1, \cdots, Y_k) \in D$. We denote $\mathbf{a} = (a_1, \cdots, a_k) \in G^k$ and

$\mathbf{b} = (b_1, \cdots, b_k) \in G^k$. Now,

$$\begin{aligned}
& \Pr[E^u(X_1) = Y_1, \cdots, E^u(X_k) = Y_k] \\
\geq\ & \Pr[E^u(X_1) = Y_1, \cdots, E^u(X_k) = Y_k \wedge \mathsf{DIST}] \\
=\ & \sum_{\mathbf{a},\mathbf{b} \in D} \Pr[E^u(a_1) = b_1, \cdots, E^u(a_k) = b_k, X_1 = a_1, Y_1 = b_1, \cdots, X_k = a_k, Y_k = b_k] \\
=\ & \sum_{\mathbf{a},\mathbf{b} \in D} \Pr[E^u(a_1) = b_1, \cdots, E^u(a_k) = b_k] \times \Pr[X_1 = a_1, Y_1 = b_1, \cdots, X_k = a_k, Y_k = b_k] \\
& \qquad \text{(since } (X_1, Y_1, \cdots, X_q, Y_q) \text{ is independent with } E^u\text{)} \\
=\ & \frac{1}{\mathbf{P}(N,k)} \times \sum_{\mathbf{a},\mathbf{b} \in D} \Pr[X_1 = a_1, Y_1 = b_1, \cdots, X_k = a_k, Y_k = b_k] \qquad \text{(using equation 1)} \\
=\ & \frac{1}{\mathbf{P}(N,k)} \times \Pr[\mathsf{DIST}] \qquad (\mathsf{DIST} \text{ is true if and only if } (X_1, \cdots, X_k), (Y_1, \cdots, Y_k) \in D) \\
\geq\ & \frac{1 - \Pr[\mathsf{COLL}_{\mathrm{in}}] - \Pr[\mathsf{COLL}_{\mathrm{out}}]}{\mathbf{P}(N,k)}. \blacksquare
\end{aligned}$$

We say a distinguisher is $(q, \sigma)$-CPA if it asks at most $q$ encryption queries such that total number of blocks in all queries is at most $\sigma$. Similarly we can define $(q, \sigma)$-CCA distinguisher where it can ask both encryption and decryption queries. Let $F : \mathcal{K} \times D \to D$ be a cipher with finite key-space $\mathcal{K}$. Suppose an oracle algorithm or distinguisher $\mathcal{A}$ has access of a cipher with domain $D$. Now $\mathcal{A}^F \Rightarrow b$ represents the event that $\mathcal{A}$ outputs $b$ after interacting with $F_K$ where $K \stackrel{*}{\leftarrow} \mathcal{K}$. Similarly we define $\mathcal{A}^{F,F^{-1}} \Rightarrow b$. The CPA advantage of oracle algorithms for a blockcipher $E : \mathcal{K} \times G \to G$ is $\mathbf{Adv}^{\mathrm{CPA}}_{\mathcal{A}}(E, E^u) = \Pr[\mathcal{A}^E \Rightarrow 1] - \Pr[\mathcal{A}^{E^u} \Rightarrow 1]$. The prp-insecurity of $E$ is $\mathbf{Insec}^{\mathrm{prp}}_E(q, \sigma) = \max_{\mathcal{A}} \mathbf{Adv}^{\mathrm{CPA}}_{\mathcal{A}}(E, E^u)$ where maximum is taken over all $(q, \sigma)$-CPA distinguishers. CCA advantage of $\mathcal{A}$ and sprp-insecurity of a blockcipher can be defined similarly. Let $\mathcal{A}^{F,F^{-1}}$ be an oracle algorithm having access of an online cipher and its inverse. Responses of an ideal online cipher or uniform random online permutation (UROP) oracle $\Pi^u$ and its inverse oracle $(\Pi^u)^{-1}$ is defined below in figure 1. Like insecurity of a blockcipher we can define $\mathbf{Insec}^{\mathrm{prop}}_F(q, \sigma)$ and $\mathbf{Insec}^{\mathrm{sprop}}_F(q, \sigma)$ where $F$ is an online cipher. It is the maximum CPA or CCA advantage for $(q, \sigma)$ distinguishers distinguishing $F$ from the ideal online cipher $\Pi^u$.

Initially $\mathbb{P} = \emptyset$ and a function $\Gamma : \mathbb{P} \to \mathsf{Perm}(G)$.

On encryption query $M \in G^m$

```
for $i = 1$ to $m$
    $p = M[1..i-1]$;
    if $p \in \mathbb{P}$ then $C[i] = \Gamma(p)(M[i])$;
    else
        $\Pi^u_p \stackrel{*}{\leftarrow} \mathsf{Perm}(G)$;
        $\mathbb{P} \leftarrow \mathbb{P} \cup \{p\}$;
        $\Gamma(p) = \Pi^u_p$;
        $C[i] = \Gamma(p)(M[i])$;
    endif
endfor
return $C = C[1..m]$;
```

On decryption query $C \in G^m$

```
for $i = 1$ to $m$
    $p = M[1..i-1]$;
    if $p \in \mathbb{P}$ then $M[i] = \Gamma(p)^{-1}(C[i])$;
    else
        $\Pi^u_p \stackrel{*}{\leftarrow} \mathsf{Perm}(G)$;
        $\mathbb{P} \leftarrow \mathbb{P} \cup \{p\}$;
        $\Gamma(p) = \Pi^u_p$;
        $M[i] = \Gamma(p)^{-1}(C[i])$;
    endif
endfor
return $M = M[1..m]$;
```

Figure 1: Responses of a UROP oracle $\Pi^u$ and its inverse oracle $(\Pi^u)^{-1}$.

The *longest common prefix* of $M, M' \in G^*$ (or $\mathsf{LCP}(M, M')$) is the block-sequence $N \in G^\ell$ such that $N$ is a longest common prefix of $M$ and $M'$. One can check that $\mathsf{LCP}(M, M')$ always exists and it is unique. The length of the longest common prefix is denoted by $\ell_{M,M'}$. Any element of the form $\tau =$

$((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{T} := ((G^+)^2)^+$ is known as *qr-tuple* or *query-response tuple*[1] where $M_i$'s and $C_i$'s are block-sequences.

A qr-tuple $\tau = ((M_1, C_1), \cdots, (M_q, C_q))$ is said to be **online-compatible** if $\ell_{M_i,M_j} = \ell_{C_i,C_j}$, for all $1 \leq i, j \leq q$. Let $\mathcal{T}_{\rm oc}$ be the set of all online-compatible qr-tuples. Let $\tau = ((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{T}_{\rm oc}$ be a qr-tuple then for any $p \in \mathbb{P}_M := \mathbb{P}(M_1, \cdots, M_q)$ we define the **corresponding block-sequence** $q^p \in \mathbb{P}_C := \mathbb{P}(C_1, \cdots, C_q)$ by $C_i[1..j]$ where $p = M_i[1..j]$[2].

Now we provide bounds of interpolation probability of UROP $\Pi^u$.

**Lemma 2.3** (Interpolation probability of UROP) *Let* $\mathbf{Pr} := \Pr[\Pi^u(M_1) = C_1, \cdots, \Pi^u(M_q) = C_q] = 0$ *where* $\Pi^u$ *is an UROP. Now* $\frac{1}{N^\sigma} \leq \mathbf{Pr} \leq \frac{1}{\mathbf{P}(N,\sigma)}$ *if* $((M_1, C_1), \cdots, (M_q, C_q))$ *is an* online-compatible*, otherwise* $\mathbf{Pr} = 0$*, where* $\sigma 0 \sigma(M_1, \cdots, M_q)$*.*

**Proof.** The first part of the lemma is clearly true since for any online permutation $f$, $((M_1, f(M_1)), \cdots, (M_q, f(M_q)))$ is online-compatible.

Now we prove the for online-compatible tuple. Let $p \in \mathbb{P} := \mathbb{P}(M_1, \cdots, M_q)$. We denote $y_p = \text{last}(q^p) = C_i[j]$ where $p = M_i[1..j]$. Now given $p_1 \neq p_2$ such that $\text{chop}(p_1) = \text{chop}(p_2)$ we have $\text{last}(p_1) \neq \text{last}(p_2)$ (since $p_1 \neq p_2$) and $y_{p_1} \neq y_{p_2}$ (since the tuple is online-compatible). Recall that $\mathbb{P}' := \mathbb{P}'(M_1, \cdots, M_q) = \{p' \in G^* : p' = \text{chop}(p), p \in \mathbb{P}\}$. Now one can see that

$$\begin{aligned}
\Pr[\Pi^u(M_1) = C_1, \cdots, \Pi^u(M_q) = C_q] &= \Pr[\Pi^u_{\text{chop}(p)}(\text{last}(p)) = y_p \quad \forall p \in \mathbb{P}(M_1, \cdots, M_q)] \\
&= \Pr[\Pi^u_{p'}(x) = y \quad \forall p' \in \mathbb{P}', p = (p', x) \in \mathbb{P}, y = y_p] \\
&= \prod_{p' \in \mathbb{P}'} \Pr[\Pi^u_{p'}(x) = y, \forall x, y, \text{ such that } p = (p', x) \in \mathbb{P}, y = y_p] \\
&\qquad\qquad \text{(since responses of } \Pi^u_{p'} \text{ independently distributed)} \\
&= \prod_{p' \in \mathbb{P}'} \frac{1}{\mathbf{P}(N, d_{p'})} \quad \text{(for each } p', \Pi^u_{p'} \text{ is URP)}
\end{aligned}$$

where $d_{p'} = |\{x : (p', x) \in \mathbb{P}\}|$ and $\sigma' = |\mathbb{P}'(M_1, \cdots, M_q)|$. Note that $\sum_{p' \in \mathbb{P}'} d_{p'} = \sigma$ and hence $\prod_{p' \in \mathbb{P}'} \frac{1}{\mathbf{P}(N,d_{p'})} \leq \frac{1}{\mathbf{P}(N,\sigma)}$. Trivially $\prod_{p' \in \mathbb{P}'} \frac{1}{\mathbf{P}(N,d_{p'})} \geq \frac{1}{N^\sigma}$. This completes the proof. ■

Now we define an important object called view or transcript[3] of a distinguisher which actually contains all query-responses in the form of tuple.

**Definition 2.1** (view or transcript of an adversary) *Let* $g : G^+ \to G^+$ *be an oracle and* $\tau = ((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{T}$*, for some* $q \geq 1$*.*

(1) Chosen Plaintext Adversary *:* $\tau$ *is called a view of* $\mathcal{A}^g$ *and denoted as* $\mathsf{view}(\mathcal{A}^g)$ *if* $M_1, \cdots, M_q$ *are all the queries made by* $\mathcal{A}$ *and* $C_1, \cdots, C_q$ *are the corresponding responses.*

(2) Chosen Ciphertext Adversary *:* $\tau$ *is called a view of* $\mathcal{A}^{g,g^{-1}}$ *and denoted as* $\mathsf{view}(\mathcal{A}^{g,g^{-1}})$*, if* $M_i$ *is the query and* $C_i$ *is the response whenever the* $i^{\rm th}$ *query is* $g$*-query or if* $C_i$ *is query and* $M_i$ *is response whenever* $i^{\rm th}$ *query is* $g^{-1}$*-query*[4]*.*

We say that a tuple $\tau := ((M_1, C_1) ,\cdots, (M_q, C_q)) \in \mathcal{T}$ is **$\mathcal{A}$-compatible** if for all $1 \leq i \leq q$, $M_i$ (or $C_i$) will be the $i^{\rm th}$ $g$-query (or $g^{-1}$-query respectively) when $(M_1, C_1),\cdots, (M_{i-1}, C_{i-1})$ are given as

[1] Later we see that the pair $(M_i, C_i)$ corresponds to a query-response pair where $M_i$ is encryption query and $C_i$ is response or $C_i$ is decryption query and $M_i$ is response.

[2] Clearly, $j = ||p||$ but there can be more than one choices of $i$. So we need to check well defined-ness of $q^p$. Suppose $p = M_i[1..j] = M_{i'}[1..j]$ for some $i, i' \leq q$ and hence $\ell_{M_i,M_{i'}} \geq j$. Since $\tau$ is online compatible, $\ell_{C_i,C_{i'}} = \ell_{M_i,M_{i'}} \geq j$. Thus, $C_i[1..j] = C_{i'}[1..j]$.

[3] the term "transcript" has been used in many literatures, but in this paper we mainly use the word view as it really signifies the view of the oracle which is obtained by the distinguisher after having query-responses.

[4] in both cases we have $g(M_i) = C_i$.

query-responses for the first $(i-1)$ queries. Clearly, a view $\mathsf{view}(\mathcal{A}^g)$ or $\mathsf{view}(\mathcal{A}^{g,g^{-1}})$ is always $\mathcal{A}$-compatible. $\mathcal{A}$-compatibility of a tuple is completely independent with oracles. Let $\tau$ be a $\mathcal{A}$-compatible tuple. Then,

$$g(M_1) = C_1, \cdots, g(M_q) = C_q \quad \text{if and only if} \quad \mathsf{view}(\mathcal{A}^{g,g^{-1}}) = \tau \text{ or } \mathsf{view}(\mathcal{A}^g) = \tau.$$

**Lemma 2.4** *Let $\tau = ((M_1, C_1)\ ,\cdots,\ (M_q, C_q))$ be a $\mathcal{A}$-compatible tuple. Then for an oracle $g$ we have,*

$$\begin{aligned}\Pr[g(M_1) = C_1, \cdots, g(M_q) = C_q] &= \Pr[\mathsf{view}(\mathcal{A}^g) = \tau] \qquad \mathcal{A} \textit{ is a CPA-distinguisher} \qquad (3)\\ &= \Pr[\mathsf{view}(\mathcal{A}^{g,g^{-1}}) = \tau] \quad \mathcal{A} \textit{ is a CCA-distinguisher} \qquad (4)\end{aligned}$$

Now we define some views, subsets of $\mathcal{T}_{\mathrm{oc}}$, called bad views and bound the probability that a bad view occurs when a distinguisher is interacting with uniform random online permutation $\Pi^u$. These bad views will be considered as bad views for the online ciphers HCBC1, HCBC2, MHCBC and MCBC. Define $x_p = \mathrm{last}(p)$ and $y_p = \mathrm{last}(q^p)$ where .

$$\begin{aligned}\mathcal{V}_{\mathrm{bad},1} &= \{\tau \in \mathcal{T}_{\mathrm{oc}} :\ y_{p_1} = y_{p_2} \ \text{ or } \ y_{p_1} = \mathbf{0}, \text{ for some } p_1 \neq p_2 \in \mathbb{P}_M\}\\ \mathcal{V}_{\mathrm{bad},2} &= \{\tau \in \mathcal{T}_{\mathrm{oc}} :\ (y_{p_1}, x_{p_1}) = (y_{p_2}, x_{p_2}) \text{ or } (y_{p_1}, x_{p_1}) = (\mathbf{0}, \mathbf{0}), p_1 \neq p_2 \in \mathbb{P}_M\}\\ \mathcal{V}_{\mathrm{bad},3} &= \{\tau \in \mathcal{T}_{\mathrm{oc}} :\ y_{p_1} + x_{p_1} = y_{p_2} + x_{p_2} \text{ or } y_{p_1} + x_{p_1} = \mathbf{0}, p_1 \neq p_2 \in \mathbb{P}_M\}.\\ \mathcal{V}_{\mathrm{bad},4} &= \{\tau \in \mathcal{T}_{\mathrm{oc}} :\ y_{p_1} + x_{p_1} = y_{p_2} + x_{p_2} \text{ or } y_{p_1} + x_{p_1} = \mathbf{0} \text{ or } \mathbf{1}, p_1 \neq p_2 \in \mathbb{P}_M\}.\end{aligned}$$

**Proposition 2.5** *For any $(q, \sigma)$ CPA-distinguisher $\mathcal{A}$ interacting with a uniform random online permutation $\Pi^u$, $\Pr[\mathsf{view}(\mathcal{A}^{\Pi}) \in \mathcal{V}_{\mathrm{bad},1}] \leq \frac{\sigma(\sigma-1)}{2N}$. For any $(q, \sigma)$ CCA-distinguisher $\mathcal{A}$ interacting with a uniform random online permutation $\Pi^u$ and its inverse $(\Pi^u)^{-1}$, $\Pr[\mathsf{view}(\mathcal{A}^{\Pi^u,(\Pi^u)^{-1}}) \in \mathcal{V}_{\mathrm{bad},i}] \leq \frac{(\sigma+2)(\sigma+3)}{N}$, $i = 2, 3, 4$.*

**Proof.** Let us consider dictionary order $\prec$ on the set of pairs $(i, j)$. Thus, $(i', j') \prec (i, j)$ if either $i' < i$ or $i = i'$ and $j' < j$.

If $\mathsf{view}(\mathcal{A}^{\Pi}) \in \mathcal{V}_{\mathrm{bad},1}$ then there must exist smallest[5] $(i, j)$ such that $C_i[j] = C_{i'}[j']$ for some $(i', j') \prec (i, j)$ or $C_i[j] = \mathbf{0}$. Since $C_i[j] = \Pi^u_{M_i[1..j-1]}(M_i[j])$ the above event holds with probability at most $\frac{1}{N-k+1}$ $(\leq \frac{k-1}{N})$ where $k$ is the number of times line 8 of figure 1 is executed till the computation of $C_i[j]$. In other words the size of $\mathbb{P}$ at the time of computation of $C_i[j]$. Note that $k$ varies from 1 to $\sigma = |\mathbb{P}(M_1, \cdots, M_q)|$. Summing over possible pairs $(i, j)$ we obtain that $\Pr[\mathsf{view}(\mathcal{A}^{\Pi}) \in \mathcal{V}_{\mathrm{bad},1}] \leq \sum_{k=1}^{\sigma} \frac{k-1}{N} \leq \frac{\sigma(\sigma-1)}{2N}$.

Note that if $\tau \in \mathcal{V}_{\mathrm{bad},4}$ then trivially $\tau \in \mathcal{V}_{\mathrm{bad},j}$ for $j = 2, 3$. Thus we need to prove only for $\tau \in \mathcal{V}_{\mathrm{bad},4}$. A similar approach as described for $\mathcal{V}_{\mathrm{bad},1}$ can be applied.

If $\mathsf{view}(\mathcal{A}^{\Pi}) \in \mathcal{V}_{\mathrm{bad},4}$ then there must exist smallest $(i, j)$ such that $M_i[j] + C_i[j] = M_{i'}[j'] + C_{i'}[j']$ for some $(i', j') \prec (i, j)$ or $M_i[j] + C_i[j] = \mathbf{0}$ or $\mathbf{1}$. Since either $C_i[j] = \Pi^u_{M_i[1..j-1]}(M_i[j])$ (if $i^{\text{th}}$ query is encryption query) or $M_i[j] = (\Pi^u)^{-1}_{C_i[1..j-1]}(C_i[j])$ (if $i^{\text{th}}$ query is decryption query) is uniformly distributed over a set of size at least $N-k+1$, the above event holds with probability at most $\frac{3}{N-k+1}$ $(\leq \frac{k+2}{N})$. Summing over possible pairs $(i, j)$ we obtain that $\Pr[\mathsf{view}(\mathcal{A}^{\Pi}) \in \mathcal{V}_{\mathrm{bad},4}] \leq \sum_{k=1}^{\sigma} \frac{k+2}{N} \leq \frac{(\sigma+2)(\sigma+3)}{2N}$. ■

**Theorem 2.6** (Strong interpolation theorem)
*Suppose $g_0$ and $g_1$ are two probabilistic oracles and $\mathcal{A}$ is a CPA or CCA distinguisher. Let $\mathcal{T}_{\mathcal{A}} = \mathcal{V}_{\mathrm{good}} \cup \mathcal{V}_{\mathrm{bad}}$. Suppose the following conditions hold.*

(1) $\Pr[g_0(M_1) = C_1, \cdots, g_0(M_q) = C_q] \geq (1 - \varepsilon_1) \times \Pr[g_1(M_1) = C_1, \cdots, g_1(M_q) = C_q]$
$\forall((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{V}_{\mathrm{good}}$.

(2) $\Pr[\mathsf{view}(\mathcal{A}^{g_1,g_1^{-1}}) \in \mathcal{V}_{\mathrm{bad}}] \leq \varepsilon_2$ *(or $\Pr[\mathsf{view}(\mathcal{A}^{g_1} \in \mathcal{V}_{\mathrm{bad}}] \leq \varepsilon_2$ when $\mathcal{A}$ is a CPA-distinguisher).*

[5] for the first time in line 8 of fig 1 the bad property holds.

*Then we have* $\mathbf{Adv}_{\mathcal{A}}(g_0, g_1) \leq \varepsilon_1 + \varepsilon_2$.

**Proof.** Here we denote $\tau = ((M_1, C_1), \cdots, (M_q, C_q))$. Now,

$$\begin{aligned}
\mathbf{Adv}_{\mathcal{A}}(g_0, g_1) &= \sum_{\tau \in \mathcal{T}_{\mathcal{A}}} (\Pr[g_0(M_1) = C_1, \cdots, g_0(M_q) = C_q] - \Pr[g_1(M_1) = C_1, \cdots, g_1(M_q) = C_q]) \\
&= \sum_{\tau \in \mathcal{V}_{\text{good}}} (\Pr[g_0(M_1) = C_1, \cdots, g_0(M_q) = C_q] - \Pr[g_1(M_1) = C_1, \cdots, g_1(M_q) = C_q]) \\
&\quad + \sum_{\tau \in \mathcal{V}_{\text{bad}}} (\Pr[g_0(M_1) = C_1, \cdots, g_0(M_q) = C_q] - \Pr[g_1(M_1) = C_1, \cdots, g_1(M_q) = C_q]) \\
&\leq \sum_{\tau \in \mathcal{V}_{\text{good}}} \varepsilon_1 \times \Pr[g_1(M_1) = C_1, \cdots, g_1(M_q) = C_q] + \Pr[\mathsf{view}(\mathcal{A}^{g_1, g_1^{-1}}) \in \mathcal{V}_{\text{bad}}] \\
&\leq \varepsilon_1 \times \Pr[\mathsf{view}(\mathcal{A}^{g_1, g_1^{-1}}) \in \mathcal{V}_{\text{good}}] + \varepsilon_2 \leq \varepsilon_1 + \varepsilon_2. \blacksquare
\end{aligned}$$

Now we state an important result which is corollary from strong interpolation theorem (see theorem 2.6), interpolation probability for UROP (see lemma 2.3) and the above proposition 2.5. This result is going to be used for obtaining bound for advantages of online ciphers considered in this paper.

**Proposition 2.7** (main tool of the paper)
*Let $F$ be an online cipher. Suppose for some $1 \leq k \leq 4$ and for all $\tau \in \mathcal{T}_{\text{oc}} \setminus \mathcal{V}_{\text{bad},i}$, the interpolation probability of $F$ satisfies the following equation*

$$\Pr[F(M_1) = C_1, \cdots, F(M_q) = C_q] \geq \frac{(1 - \varepsilon)}{\mathbf{P}(N, \sigma)} \tag{5}$$

*where $\tau = ((M_1, C_1), \cdots, (M_q, C_q))$ and $\sigma$ is the total number of blocks in $q$ plaintexts. Then $F$ is $(q, \sigma, \varepsilon + \frac{(\sigma+2)(\sigma+3)}{2N})$-CCA secure when $i = 2, 3, 4$ or $F$ is $(q, \sigma, \varepsilon + \frac{\sigma(\sigma-1)}{2N})$-CPA secure when $i = 1$.*

# 3 Two known online ciphers : HCBC1 and HCBC2

## 3.1 HCBC1 [1]

Given a permutation $\pi \in \mathsf{Perm}(G)$ and a hash function $h : G \to G$, we define $\mathsf{HCBC1}[\pi, h]$ online permutation. Let $x_i, y_i \in G$, $1 \leq i \leq m$, $y_0 = \mathbf{0}$. Now,

$$\mathsf{HCBC1}[\pi, h](x_1, \cdots, x_m) = (y_1, \cdots, y_m),\ y_i = \pi(h(y_{i-1}) + x_i),\ 1 \leq i \leq m.$$

Note that $\mathsf{HCBC1}[\pi, h]$ is an online permutation. The online property can be proved by induction as the $i^{\text{th}}$ output block only depends on $(i-1)^{\text{th}}$ output block and $i^{\text{th}}$input block. It is also a permutation and its inverse is defined as

$$\mathsf{HCBC1}[\pi, h]^{-1}(y_1, \cdots, y_m) = (x_1, \cdots .x_m),\ x_i = \pi^{-1}(y_i) - h(y_{i-1}),\ 1 \leq i \leq m.$$

Let $E^u \xleftarrow{*} \mathsf{Perm}(G)$ be a URP or uniform random permutation, $e \xleftarrow{*} E$ be a block cipher and $\mathsf{h} \xleftarrow{*} H$ be an $\varepsilon$-$\Delta$universal hash function from $G$ to $G$. We define $\mathsf{H1} := \mathsf{HCBC1}[E^u, \mathsf{h}]$, $\mathsf{H1}' := \mathsf{HCBC1}[e, \mathsf{h}]$.

### Interpolation probability of $\mathsf{H1}$

We compute $q$-interpolation probability of $\mathsf{H1}$ for a type-1 qr-tuple $\tau := ((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{V}_{\text{good},1}$, i.e., we compute $\Pr[\mathsf{H1}(M_1) = C_1, \cdots, \mathsf{H1}(M_q) = C_q]$.

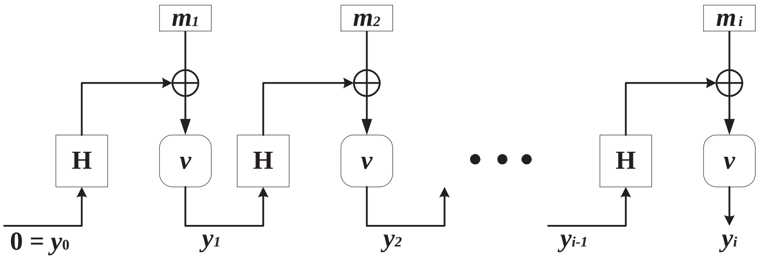

Figure 2: Hash-CBC online function $\mathsf{HCBC1}[e, \mathsf{h}]$ where the underlying group is $(\{0,1\}^n, \oplus)$.

From the definition of $\mathsf{HCBC1}$ one can verify the following equivalences.

$$\begin{aligned} & \mathsf{H1}(M_1) = C_1, \cdots, \mathsf{H1}(M_q) = C_q \\ \Leftrightarrow\quad & b^{\mathsf{H1}}(M_i[1..j]) = C_i[j],\ \ 1 \le j \le \|M_i\|,\ 1 \le i \le q \\ \Leftrightarrow\quad & E^u(\ \mathsf{h}(\mathrm{last}(q^{\mathrm{chop}(p)})) + \mathrm{last}(p)\ ) = \mathrm{last}(q^p)\ \ \forall p \in \mathbb{P}_M \end{aligned}$$

Thus while computing the interpolation we have $(\mathsf{h}(\mathrm{last}(q^{\mathrm{chop}(p)})) + \mathrm{last}(p))_{p\in\mathbb{P}_M}$ corresponding to the all inputs of $E^u$ and $(\mathrm{last}(q^p))_{p\in\mathbb{P}_M}$ corresponding to the all outputs of $E^u$. Since $\tau \in \mathcal{V}_{\mathrm{good},1}$, $\mathrm{last}(q^p)$'s are distinct for all $p \in \mathbb{P}_M$. Thus, all outputs of $E^u$ are distinct. Now we prove that for all $p \in \mathbb{P}_M$, $(\mathrm{last}(q^{\mathrm{chop}(p)}), \mathrm{last}(p))$'s are distinct. Suppose for some $p_1, p_2$, $(\mathrm{last}(q^{p'_1}), \mathrm{last}(p_1)) = (\mathrm{last}(q^{p'_2}), \mathrm{last}(p_2))$ where $p'_i = \mathrm{chop}(p_i)$. Now $\mathrm{last}(q^{p'_1}) = \mathrm{last}(q^{p'_2})$ implies that $p'_1 = p'_2$ and hence $p_1 = p_2$ (since $\mathrm{last}(p_1) = \mathrm{last}(p_2)$). By using lemma 2.1 we have $\Pr[(\mathsf{h}(\mathrm{last}(q^{\mathrm{chop}(p)})) + \mathrm{last}(p))\text{'s are distinct}] \ge 1 - \varepsilon\binom{\sigma}{2}$. Thus, all inputs of $E^u$ are distinct with probability at least $1-\varepsilon\binom{\sigma}{2}$. Moreover, the inputs and outputs are independent with $E^u$ since $\mathsf{h}$ is independent with $E^u$. So $\Pr[E^u(\ \mathsf{h}(\mathrm{last}(q^{\mathrm{chop}(p)}))+\mathrm{last}(p)\ ) = \mathrm{last}(q^p)\ \forall p \in \mathbb{P}_M] \ge \frac{1-\varepsilon\binom{\sigma}{2}}{\mathbf{P}(N,\sigma)}$.

Recall that, $\tau$ is type-1 qr tuple i.e., $\tau \in \mathcal{V}_{\mathrm{good},1}$ if for all $p \in \mathbb{P}^* = \mathbb{P}_M \cup \{\lambda\}$, $\mathrm{last}(q^p)$'s are distinct. Note that $q^\lambda = \lambda$, $\mathrm{last}(\lambda) = \mathbf{0}$ and $q^p = C_i[1..j]$ where $p = M_i[1..j]$. $\mathbb{P}_M$ is the set of non-empty prefixes of $\{M_1, \cdots, M_q\}$ and $\mathbb{P}'_M = \{p' : p' = \mathrm{chop}(p), p \in \mathbb{P}_M\}$,

**Theorem 3.1** (interpolation probability of HCBC1)

$$\Pr[\mathsf{H1}(M_1) = C_1, \cdots, \mathsf{H1}(M_q) = C_q] \ge \frac{1 - \varepsilon\binom{\sigma}{2}}{\mathbf{P}(N,\sigma)}\ \ \forall((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{V}_{\mathrm{good},1} \tag{6}$$

**Corollary 3.2** *Let $\mathcal{A}$ be a $(q, \sigma)$-CPA distinguisher then we have*

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{CPA}}(\mathsf{H1}) \le \binom{\sigma}{2}(\varepsilon + \frac{1}{N}),$$

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{CPA}}(\mathsf{H1}') \le \binom{\sigma}{2}(\varepsilon + \frac{1}{N}) + \mathbf{Insec}_{E}^{\mathrm{CPA}}(\sigma)$$

*where $\mathsf{H1}$ is based on $\varepsilon$-$\Delta$universal hash function. If we consider the finite field multiplication based universal hash function then $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{CPA}}(\mathsf{H1}') \le \frac{\sigma(\sigma-1)}{N} + \mathbf{Insec}_{E}^{\mathrm{CPA}}(\sigma)$.*

## 3.2 HCBC2 [1]

Now we make similar study for $\mathsf{HCBC2}$. We follow same notations as given in HCBC1 except that $h : G^2 \to G$, $\mathsf{h}$ is $\varepsilon$-$\Delta$universal hash from $G^2$ to $G$ and $x_0 = \mathbf{0}$. $\mathsf{H2} := \mathsf{HCBC2}[E^u, \mathsf{h}]$, $\mathsf{H2}' := \mathsf{HCBC2}[e, \mathsf{h}]$ where

$$\mathsf{HCBC2}[\pi, h](x_1, \cdots, x_m) = (y_1, \cdots, y_m),\ \ y_i = \pi(h(x_{i-1}, y_{i-1}) + x_i) + h(x_{i-1}, y_{i-1}),\ 1 \le i \le m.$$

$$\mathsf{HCBC2}[\pi, h]^{-1}(y_1, \cdots, y_m) = (x_1, \cdots .x_m),\ \ x_i = \pi^{-1}(y_i - h(x_{i-1}, y_{i-1})) - h(x_{i-1}, y_{i-1}),\ 1 \le i \le m.$$

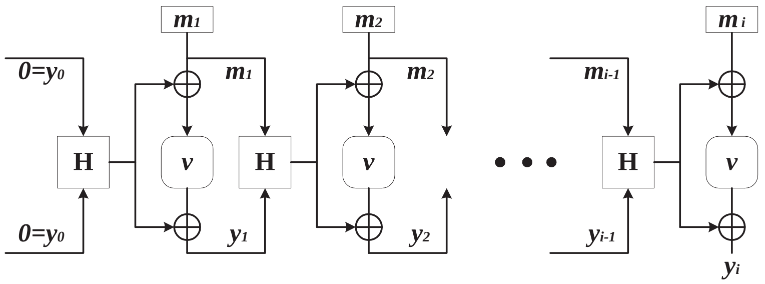

Figure 3: Hash-CBC online function $\mathsf{HCBC2}[e, \mathsf{h}]$ where the underlying group is $(\{0,1\}^n, \oplus)$.

**Interpolation probability of $\mathsf{H2}$**

We compute $q$-interpolation probability of $\mathsf{H2}$ for any given type-2 qr-tuple $\tau := ((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{V}_{\text{good},2}$. From the definition of $\mathsf{HCBC2}$ we have the following equivalences.

$$\begin{aligned} & \mathsf{H2}(M_1) = C_1, \cdots, \mathsf{H1}(M_q) = C_q \\ \Leftrightarrow \quad & E^u(z_{\text{chop}(p)} + \text{last}(p)\ ) = \text{last}(q^p) + z_{\text{chop}(p)} \ \ \forall p \in \mathbb{P}_M \end{aligned}$$

where $z_p = \mathsf{h}(\text{last}(p), \text{last}(q^p))$. Thus while computing the interpolation, $(z_{\text{chop}(p)} + \text{last}(p))_{p \in \mathbb{P}_M}$ are all inputs of $E^u$ and $(z_{\text{chop}(p)} + \text{last}(q^p))_{p \in \mathbb{P}_M}$ are all outputs of $E^u$. Since $\tau \in \mathcal{V}_{\text{good},2}$, by using a similar argument, as given for $\mathcal{V}_{\text{good},1}$, we can show that $((\text{last}(\text{chop}(p)), \text{last}(q^{\text{chop}(p)})), \text{last}(p))$'s are distinct and $((\text{last}(\text{chop}(p)), \text{last}(q^{\text{chop}(p)})), \text{last}(q^p))$'s are distinct for all $p \in \mathbb{P}_M$. By using lemma 2.1 we have

$$\Pr[z_{\text{chop}(p)} + \text{last}(p))\text{'s are distinct}] \geq 1 - \varepsilon \binom{\sigma}{2}$$

$$\Pr[z_{\text{chop}(p)} + \text{last}(q^p))\text{'s are distinct}] \geq 1 - \varepsilon \binom{\sigma}{2}.$$

Thus, all inputs and outputs of $E^u$ are distinct with probability at least $1 - 2\varepsilon\binom{\sigma}{2}$ and the inputs and outputs are independent with $E^u$ (since $\mathsf{h}$ is independent with $E^u$). So by applying the proposition 2.2, $\Pr[E^u(z_{\text{chop}(p)} + \text{last}(p)\ ) = \text{last}(q^p) + z_{\text{chop}(p)} \ \ \forall p \in \mathbb{P}_M] \geq \frac{1 - 2\varepsilon\binom{\sigma}{2}}{\mathbf{P}(N,\sigma)}$.

**Theorem 3.3** (interpolation probability of HCBC2)

$$\Pr[\mathsf{H2}(M_1) = C_1, \cdots, \mathsf{H2}(M_q) = C_q] \geq \frac{1 - 2\varepsilon\binom{\sigma}{2}}{\mathbf{P}(N,\sigma)} \quad \forall((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{V}_{\text{good},2} \tag{7}$$

**Corollary 3.4** *Let $\mathcal{A}$ be a $(q,\sigma)$-CCA distinguisher then we have*

$$\mathbf{Adv}_{\mathcal{A}}^{\text{CCA}}(\mathsf{H2}) \leq \binom{\sigma}{2}(2\varepsilon + \frac{1}{N}),$$

$$\mathbf{Adv}_{\mathcal{A}}^{\text{CCA}}(\mathsf{H2}') \leq \binom{\sigma}{2}(2\varepsilon + \frac{1}{N}) + \mathbf{Insec}_{E}^{\text{CCA}}(\sigma)$$

*where $\mathsf{H2}$ is based on $\varepsilon$-$\Delta$universal hash function. If we consider the finite field multiplication based universal hash function then $\mathbf{Adv}_{\mathcal{A}}^{\text{CCA}}(\mathsf{H2}') \leq \frac{3\sigma(\sigma-1)}{2N} + \mathbf{Insec}_{E}^{\text{CCA}}(\sigma)$.*

# 4 Two new online ciphers : MHCBC and MCBC

## 4.1 MHCBC

With the same notation as in HCBC1 we define

$$\mathsf{MHCBC}[\pi, h](x_1, \cdots, x_m) = (y_1, \cdots, y_m),\ y_i = \pi(h(x_{i-1} + y_{i-1}) + x_i) + h(x_{i-1} + y_{i-1}),\ 1 \le i \le m$$

$$\mathsf{MHCBC}[\pi, h]^{-1}(y_1, \cdots, y_m) = (x_1, \cdots, x_m),\ x_i = \pi^{-1}(y_i - h(x_{i-1} + y_{i-1})) - h(x_{i-1} + y_{i-1}),\ 1 \le i \le m.$$

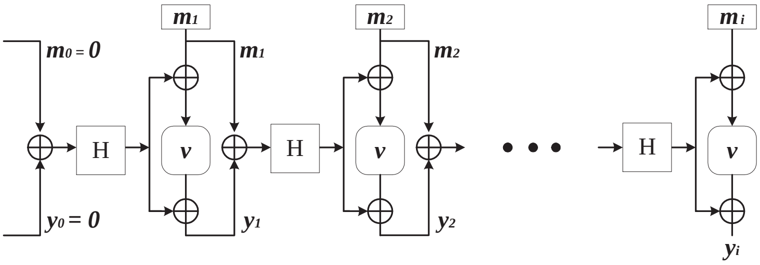

Figure 4: MHCBC or Modified-Hash CBC online cipher

$\mathsf{H3} := \mathsf{MHCBC}[E^u, \mathsf{h}]$.

$\mathsf{H3}' := \mathsf{MHCBC}[e, \mathsf{h}]$.

Note that MHCBC uses $(G, G)$ universal hash function similar to HCBC1 and still it is CCA-secure. This is true since both plaintext and ciphertext blocks are xored and hence the adversary does not have any control on the XOR. In case of HCBC2, these two blocks are inputs of a $(G^2, G)$ universal hash function.

Now we will compute interpolation probability for type-3 qr tuples $\mathcal{V}_{\text{good},3}$. Recall that a qr-tuple $((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{V}_{\text{good},3}$ if and only if $(\text{last}(p) + \text{last}(q^p))$'s are distinct for all $p \in \mathbb{P} \cup \{\lambda\}$. Basic idea of the computation pf interpolation is similar for online cipher constructions considered here. We first provide an equivalent representation of interpolation as interpolation of URP and hence it is sufficient to calculate interpolation probability of URP for a specific tuple. Then we calculate the probability that all inputs and outputs of URP. Finally by using proposition 2.2 we have interpolation probability.

**Theorem 4.1** (interpolation probability of MHCBC)

$$\Pr[\mathsf{H3}(M_1) = C_1, \cdots, \mathsf{H3}(M_q) = C_q] \ge \frac{1 - \varepsilon\binom{2\sigma}{2}}{\mathbf{P}(N, \sigma)} \quad \forall((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{V}_{\text{good},3} \tag{8}$$

**Proof.**

- ◇ From the definition of $\mathsf{HCBC3}$ we have the following equivalences.

  $$\begin{aligned} & \mathsf{H3}(M_1) = C_1, \cdots, \mathsf{H3}(M_q) = C_q \\ \Leftrightarrow\quad & E^u(z_{\text{chop}(p)} + \text{last}(p)\ ) = \text{last}(q^p) + z_{\text{chop}(p)} \ \ \forall p \in \mathbb{P}_M \end{aligned}$$

  where $z_p = \mathsf{h}(\text{last}(p) + \text{last}(q^p))$. Thus while computing the interpolation, $(z_{\text{chop}(p)} + \text{last}(p))_{p \in \mathbb{P}_M}$ are all inputs of $E^u$ and $(z_{\text{chop}(p)} + \text{last}(q^p))_{p \in \mathbb{P}_M}$ are all outputs of $E^u$.

- ◇ $((\text{last}(\text{chop}(p)) + \text{last}(q^{\text{chop}(p)})), \text{last}(p))$'s and $((\text{last}(\text{chop}(p)) + \text{last}(q^{\text{chop}(p)})), \text{last}(q^p))$'s are distinct for all $p \in \mathbb{P}_M$ (since $\tau \in \mathcal{V}_{\text{good},3}$). By using lemma 2.1 we have

  $$\Pr[z_{\text{chop}(p)} + \text{last}(p))\text{'s are distinct}] \ge 1 - \varepsilon\binom{\sigma}{2}$$

$$\Pr[z_{\mathrm{chop}(p)} + \mathrm{last}(q^p))\text{'s are distinct}] \geq 1 - \varepsilon\binom{\sigma}{2}.$$

Thus, all inputs and outputs of $E^u$ are distinct with probability at least $1 - 2\varepsilon\binom{\sigma}{2}$ and these are independent with $E^u$ (since $\mathsf{h}$ is independent with $E^u$). So by applying the proposition 2.2, $\Pr[E^u(z_{\mathrm{chop}(p)} + \mathrm{last}(p)\ ) = \mathrm{last}(q^p) + z_{\mathrm{chop}(p)}\ \ \forall p \in \mathbb{P}_M] \geq \frac{1-2\varepsilon\binom{\sigma}{2}}{\mathbf{P}(N,\sigma)}$. ■

**Corollary 4.2** *Let $\mathcal{A}$ be a $(q,\sigma)$-CCA distinguisher then we have*

$$\mathbf{Adv}^{\mathrm{CCA}}_{\mathcal{A}}(\mathsf{H3}) \leq \binom{\sigma}{2}(2\varepsilon + \frac{1}{N}),$$

$$\mathbf{Adv}^{\mathrm{CCA}}_{\mathcal{A}}(\mathsf{H3}') \leq \binom{\sigma}{2}(2\varepsilon + \frac{1}{N}) + \mathbf{Insec}^{\mathrm{CCA}}_{E}(\sigma)$$

*where* H3 *is based on $\varepsilon$-$\Delta$universal hash function. If we consider the finite field multiplication based universal hash function then $\mathbf{Adv}^{\mathrm{CCA}}_{\mathcal{A}}(\mathsf{H3}') \leq \frac{3\sigma(\sigma-1)}{2N} + \mathbf{Insec}^{\mathrm{CCA}}_{E}(\sigma)$.*

## 4.2 MCBC or modified-CBC

A simple replacement of $H$ of MHCBC by $v$ (note that, from example 2.2 we know that $v$ is universal hash function) would not make CCA-secure. So define $\mathsf{H'3}(x_1,\cdots,x_m) = (y_1,\cdots,y_m)$ where $y_i = \pi(\pi(x_{i-1} + y_{i-1}) + x_i) + \pi(x_{i-1} + y_{i-1})$, $1 \leq i \leq m$. It is easy to see that $\mathsf{H'3}^{-1}(\mathbf{0}) = v(\mathbf{0}) = v_0$ (known to us) and hence $\mathsf{H'3}(\mathbf{0}) = v_0 \oplus v(v_0)$. So $v(v_0)$ is also known to us and call it $v_1$. Now, $\mathsf{H'3}(v_0, v_1) = (0, v_1 \oplus v_0)$ always true where this is true with probability close to $1/N$ for the ideal online cipher. Thus we can have CCA-attack by making only three queries with four blocks.

Let $\pi \in \mathsf{Perm}(G)$ then we define MCBC or modified CBC online permutation as follows :

$$\mathsf{MHCBC}[\pi](x_1,\cdots,x_m) = (y_1,\cdots,y_m),\ y_i = \pi(\pi(x_{i-1} + y_{i-1}) + x_i) + K + x_i,\ 1 \leq i \leq m$$

where $K = \pi(\mathbf{1})$. We write $\mathsf{MC} := \mathsf{MCBC}[E^u]$ and $\mathsf{MC}' := \mathsf{MCBC}[e]$ for a chosen block cipher $e \overset{*}{\leftarrow} E$.

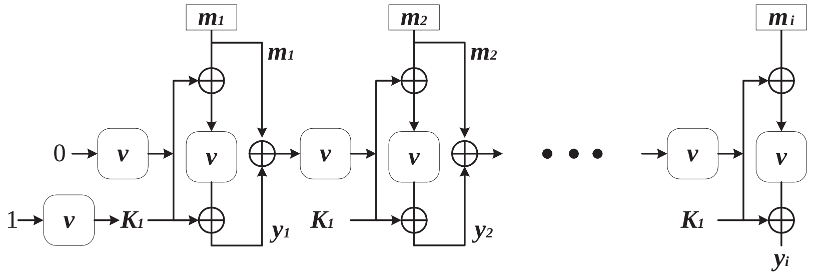

Figure 5: MCBC or Modified-CBC online cipher

MCBC does not use any universal hash function since the underlying block cipher is used in the place of the universal of hash function. Thus we are able to remove extra key storage as well as an extra design of universal hash function. The proof idea for MCBC is similar to MHCBC except the fact that we have to consider all inputs and outputs of the underlying block ciphers. We have to be little bit careful while computing interpolation probability. We first see all inputs and outputs of the uniform random permutation $E^u$ during the computations of interpolation probability of $\mathsf{MC}(M_1) = C_1, \cdots, \mathsf{MC}(M_q) = C_q$ where $((M_1, C_1), \cdots (M_q, C_q)) \in \mathcal{V}_{\mathrm{good},4}$. Let $\mathbb{P} := \mathbb{P}(M_1, \cdots, M_q)$. Now one can check that

1. $K := E^u(\mathbf{1}),\ z_{\mathrm{chop}(p)} := E^u(w_{\mathrm{chop}(p)})$ and $(\mathrm{last}(q^p) - K - z_{\mathrm{chop}(p)})$ are all outputs of $E^u,\ \ p \in \mathbb{P}_M$ where $w_p := \mathrm{last}(p) + \mathrm{last}(q^p)$.

2. $\mathbf{0}, \mathbf{1},\ w_p,\ z_{\mathrm{chop}(p)} + \mathrm{last}(p),\ p \in \mathbb{P}_M$ are all inputs of $E^u$.

Since $((M_1, C_1), \cdots (M_q, C_q)) \in \mathcal{V}_{\mathrm{good},4}$, for all $p \in \mathbb{P} \cup \{\lambda\}$, $(\mathrm{last}(p) + \mathrm{last}(q^p))$'s are distinct and different from $\mathbf{1}$. All inputs and outputs are completely determined once $z_p$ and $K$ is defined. Let $A$ be the number of possible values of $z_p$ and $K$ such that

$$\mathbf{1},\ w_p,\ z_{\mathrm{chop}(p)} + \mathrm{last}(p),\ p \in \mathbb{P}_M \text{ are distinct and}$$
$$K,\ z_{\mathrm{chop}(p)},\ \mathrm{last}(q^p) - K - z_{\mathrm{chop}(p)}\ p \in \mathbb{P}_M \text{ are distinct .}$$

We estimate $A$ by counting the complement. The above conditions are not true due to following possibilities. Recall that $\sigma' = |\mathbb{P}'|$.

1. $w_p = \mathbf{1}$ or $w_{p_1} = w_{p_2}$ for some $p_1 \neq p_2 \in \mathbb{P}'$ and $p \in \mathbb{P}$. This is not possible since $((M_1, C_1), \cdots (M_q, C_q)) \in \mathcal{V}_{\mathrm{good},4}$.

2. $z_{\mathrm{chop}(p_1)} + \mathrm{last}(p_1) = w_{p_2}$ or $z_{\mathrm{chop}(p_1)} + \mathrm{last}(p_1) = \mathbf{1}$ for some $p_1 \neq p_2,\ p_1 \in \mathbb{P}, p_2 \in \mathbb{P}'$. There are at most $N^{\sigma'} \times \sigma \times (\sigma' + 1) (\leq N^{\sigma'} \times \sigma^2)$ solutions.

3. Similarly, $z_{\mathrm{chop}(p_1)} + \mathrm{last}(p_1) = z_{\mathrm{chop}(p_2)} + \mathrm{last}(p_2)$ for some $p_1 \neq p_2 \in \mathbb{P}$. There are at most $N^{\sigma'} \times \sigma^2$ solutions.

4. $z_{\mathrm{chop}(p)}$ and $K$ are not distinct. There are at most $N^{\sigma'} \times \sigma^2$ solutions.

5. $K$ or $z_{\mathrm{chop}(p_1)}$ is same as $\mathrm{last}(q^{p_2}) - K - z_{\mathrm{chop}(p_2)}$ for some $p_1 \neq p_2 \in \mathbb{P}$. There are $N^{\sigma'} \times \sigma^2$ solutions.

6. $(\mathrm{last}(q^p) - K - z_{\mathrm{chop}(p)})$'s are not distinct. There are $N^{\sigma'} \times \sigma^2$ solutions.

So there are $5N^{\sigma'}\sigma^2$ cases where the above is not true. Thus the number of possible solutions is at least $N^{\sigma'+1} - 5N^{\sigma'}\sigma^2$ and hence $A \geq N^{\sigma'+1}(1 - \frac{5\sigma^2}{N})$. For each such solution of $z_{\mathrm{chop}(p)}$ and $K$ such that the above is true we have

$$\Pr[E^u(\mathbf{1}) = K, E^u(w_p) = z_p, E^u(z_{\mathrm{chop}(p)} + \mathrm{last}(p)) = \mathrm{last}(q^p) - K - w_{\mathrm{chop}(p)},\ \forall p \in \mathbb{P}_M] = \frac{1}{\mathbf{P}(N, \sigma + \sigma' + 1)}.$$

Summing over $A$ solutions we have

$$\begin{aligned} \Pr[\mathsf{MC}(M_1) = C_1, \cdots, \mathsf{MC}(M_q) = C_q] &\geq \frac{A}{\mathbf{P}(N, \sigma + \sigma' + 1)} \\ &\geq \frac{N^{\sigma'+1}(1 - \frac{5\sigma^2}{N})}{\mathbf{P}(N, \sigma + \sigma' + 1)} \\ &\geq \frac{(1 - \frac{5\sigma^2}{N})}{\mathbf{P}(N, \sigma)}. \end{aligned}$$

Thus we have the following main theorem for MCBC.

**Theorem 4.3** (interpolation probability of $\mathsf{MCBC}$)

$$\Pr[\mathsf{MC}(M_1) = C_1, \cdots, \mathsf{MC}(M_q) = C_q] \geq \frac{1 - 5\sigma^2/N}{\mathbf{P}(N, \sigma)} \quad \forall ((M_1, C_1), \cdots, (M_q, C_q)) \in \mathcal{V}_{\mathrm{good},4} \tag{9}$$

**Corollary 4.4** *Let $\mathcal{A}$ be a $(q, \sigma)$-CCA distinguisher then we have*

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{CCA}}(\mathsf{MC}) \leq \frac{11\sigma^2}{2N},$$

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{CCA}}(\mathsf{MC}') \leq \frac{11\sigma^2}{2N} + \mathbf{Insec}_{E}^{\mathrm{CCA}}(2\sigma).$$

# 5 Conclusion

In this paper we analyze known online ciphers namely HCBC1 and HCBC2 and propose two new online ciphers MHCBC and MCBC which have several advantages over the previous ones. In particular, MHCBC is more efficient than HCBC2 and still has CCA-security. MCBC online cipher does not need any universal hash function and hence it has better performance as well as smaller key size. Our security analysis is somewhat different from the usual game based security analysis. We believe that our proof technique would be useful in many areas where indistinguishability is concerned. One of the research goal we can think is to provide online ciphers for incomplete plaintext blocks. One can analyze the hardware performance of all these online ciphers.

**Acknowledgement.** We would like to acknowledge Professor Palash Sarkar who had inspired us to write this paper. We also would like to thank anonymous reviewers whose comments helped us to modify our earlier draft.

# References

[1] M. Bellare, A. Boldyreva, L. Knudsen and C. Namprempre. On-Line Ciphers and the Hash-CBC constructions. Advances in Cryptology - CRYPTO 2001. Lecture Notes in Computer Science, Volume **2139**, pp 292-309.

[2] M. Bellare, A. Boldyreva, L. Knudsen and C. Namprempre. On-Line Ciphers and the Hash-CBC Constructions. Cryptology eprint archive, `http://eprint.iacr.org/2007/197`.

[3] M. Bellare, J. Killan and P. Rogaway. The security of the cipher block chanining Message Authentication Code. Advances in Cryptology - CRYPTO 1994. Lecture Notes in Computer Science, Volume **839**, pp 341-358.

[4] Daniel J. Bernstein. A short proof of the unpredictability of cipher block chaining (2005). URL: http://cr.yp.to/papers.html#easycbc.

[5] J. Black and P. Rogaway. CBC MACs for arbitrary length messages. Advances in Cryptology - CRYPTO 2000. Lecture Notes in Computer Science, Volume **1880**, pp 197-215.

[6] J. Daemen and V. Rijmen. Resistance Against Implementation Attacks. A Comparative Study of the AES Proposals. In Proceedings of the Second AES Candidate Conference (AES2), Rome, Italy, March 1999. Available at http://csrc.nist.gov/encryption/aes/aes_ home.htm.

[7] Alison L. Gibbs and Francis Edward Su. On Choosing and Bounding Probability Metrics, Jan 2002.

[8] L. Knudsen. Block chaining modes of operation. Symmetric Key Block Cipher Modes of Operation Workshop, `http://csrc.nist.gov/encryption/modes/workshop1/`, Oct. 2000.

[9] H. Krawczyk. LFSR-based hashing and authenticating. Advances in Cryptology, CRYPTO 1994, Lecture Notes in Computer Science, Volume **839**, pp 129-139, Springer-Verlag 1994.

[10] M. Luby and C. Rackoff. How to construct pseudo-random permutations from pseudo-random functions. Advances in Cryptology, CRYPTO' 85, Lecture Notes in Computer Science, Volume **218**, pp 447, Springer-Verlag 1985.

[11] C. Meyer and Matyas. A new direction in Computer Data Security. John Wiley & Sons, 1982.

[12] M. Nandi. A Simple and Unified Method of Proving Indistinguishability. Indocrypt 2006, Lecture Notes in Computer Science, Volume **4329**, pp 317-334.

[13] M. Nandi. Two New Efficient CCA-Secure Online Ciphers: MHCBC and MCBC. eprint archive http://eprint.iacr.org/2008/xxx.

[14] W. Nevelsteen and B. Preneel. Software performance of universal hash functions. Advances in Cryptology, EUROCRYPT '99, Lecture Notes in Computer Science, Volume **1592**, pp 24-41, Springer-Verlag 1999.

[15] P. Rogaway. Bucket Hashing and Its Application to Fast Message Authentication. Advances in Cryptology, CRYPTO 1995, Lecture Notes in Computer Science, Volume **963**, pp 29-42, Spronger-Verlag, 1995.

[16] D. R. Stinson. On the connections between universal hashing, combinatorial designs and error-correcting codes. Congressus Numerantium **114**, 1996, pp 7-27.

[17] S. Vaudenay. Decorrelation : A Theory for Block Cipher Security. Journal of Cryptology, vol **16**, no 4/sep, 2003, pp 249-286.