Revisiting Turning Online Cipher Off

Ritam Bhaumik and Mridul Nandi
Indian Statistical Institute, Kolkata

bhaumik.ritam@gmail.com mridul.nandi@gmail.com

August 15, 2015

Abstract

In [1], a class of constructions was defined based on layers of secure online ciphers interleaved with simple mixing layers (like reversing and block-shifting). Here we show that an SPRP construction proposed in the work cited is insecure. Howevewr, the same construction is secure under the assumption that the underlying construction is online-but-last ciphers. We include a simpler proof for beyond-birthday security of other constructions proposed in the same work.

1 Introduction

Online ciphers can process plaintexts on the fly, outputting a ciphertext block as soon as the corresponding plaintext block is processed. This makes them a very useful option in many situations where the efficiency of real-time encryption is necessary. ECB and CBC (specified as a mode of operation in [7]) are early examples of online ciphers, and more sophisticated examples can be found in [2] and [6]. However, there are other situations which demand SPRP [3] security. To avoid designing an SPRP from scratch as a new primitive, [1] suggests using two or more passes of a secure online cipher, interleaved with simple publicly known blockwise-linear mixing layers. Here we examine some of the results in [1]. Of other ways of using multiple passes of an online cipher for SPRP security, [4] serves as an example.

Let $\mathcal{E}$ be a secure online cipher, $\mathcal{E}'$ be a secure online-but-last cipher, and rev be a blockwise-reversing layer. Our main results are summarised below:

- [1] claims that $\mathcal{E} \circ \mathsf{rev} \circ \mathcal{E}$ is SPRP secure. We disprove this, by providing a 4-query SPRP attack.

- We show that $\mathcal{E}' \circ \mathsf{rev} \circ \mathcal{E}'$ is SPRP secure upto the birthday bound.
- We state a simple method of obtaining a online-but-last security from online security.
- [1] shows that $\mathcal{E} \circ \mathsf{rev} \circ \mathcal{E} \circ \mathsf{rev} \circ \mathcal{E}$ achieves beyond-birthday security against an SPRP adversary. We provide a simpler proof of this result, and obtain cleaner bounds.
- Finally, [1] shows that $\mathcal{E} \circ \mathsf{rev} \circ \mathcal{E} \circ \mathsf{rev} \circ \mathcal{E}$ achieves an even better SPRP security when all plaintexts are at least $2m$ blocks long. Once again we provide a simpler proof of this result (through a minor modification of the former proof), and obtain cleaner bounds.

2 Preliminaries, Notation and Definitions

For a set A, $\#A$ will denote its size. We'll write N to denote 2^n, the number of different blocks possible, n being the number of bits in one block. For integers i and j, with $0 \leq i \leq j$, P_j^i will denote $\frac{i!}{(i-j)!}$, the number of permutations of i objects taken j at a time. (Note that the word permutation will later on be used in a different sense, to be defined.)

Prefixes Let $\mathcal{B} = \{0,1\}^n$ denote the block-space. Then $\mathcal{B}^* = \cup_0^\infty \mathcal{B}^i$ denotes all finite block-strings, called **words**. For a word $\mathbf{x}$, $||\mathbf{x}||$ will denote the number of blocks in $\mathbf{x}$. Given words $\mathbf{x}$ and $\mathbf{y}$, $\mathbf{z} = \mathbf{xy}$ denotes the **concatenation** of $\mathbf{x}$ and $\mathbf{y}$. For a word $\mathbf{z}$ and a block b, $\mathbf{z}b$ will denote the concatenation of $\mathbf{z}$ with the word containing b as its only block. $\mathbf{x}$ is called a **prefix** of $\mathbf{z}$, if $\mathbf{z} = \mathbf{xy}$ for some $\mathbf{y}$. Given a set T of words, $\mathcal{P}(T)$ will denote the set of all prefixes of all words in T. When $\mathbf{w}$ has at least j blocks, $\mathbf{w}_{1..j}$ denotes the j-block prefix of $\mathbf{w}$. More generally, $\mathbf{w}_{j_1..j_2}$ will denote the $(j_2 - j_1 + 1)$-block contiguous subword of $\mathbf{w}$ beginning in the j_1-th block and ending in the j_2-th block. Finally, for a word $\mathbf{w}$, $\mathbf{w}^R$ will denote its block-wise reverse.

Online Permutations A **permutation** $\mathcal{E}$ on $\mathcal{B}^*$ is a length-preserving bijection from $\mathcal{B}^*$ to itself. $\mathcal{E}$ is called an **online permutation** if $\mathcal{E}(\mathbf{x})$ is a prefix of $\mathcal{E}(\mathbf{y})$ if and only if $\mathbf{x}$ is a prefix of $\mathbf{y}$. $\mathcal{E}$ is called an **online-but-last permutation** if for any j, and for any words $\mathbf{x}$ and $\mathbf{y}$ each having $j+1$ or more blocks, $\mathcal{E}(\mathbf{x})_{1..j} = \mathcal{E}(\mathbf{x})_{1..j}$ if and only if $\mathbf{x}_{1..j} = \mathbf{x}_{1..j}$, i.e., it behaves as an online permutation with the (possible) exception of the last block. (Thus, an online permutation is always online-but-last.) The various permutations we will consider will generally belong to keyed families of permutations, called **ciphers**.

Security Notions For any set $\mathcal{S}$, an object $X \in \mathcal{S}$ is said to be **pseudorandom** if X cannot be efficiently distinguished from an object Y sampled uniformly from $\mathcal{S}$. That is, an efficient adversary $\mathcal{A}$ who is allowed to make finitely many queries to the oracle cannot determine with a significantly high advantage whether the oracle represents X or Y. (Y is called an ideal random object of $\mathcal{S}$.) Thus we can have pseudorandom permutations, pseudorandom online permutations and pseudorandom online-but-last permutations. (We'll often say **secure** to mean pseudorandom.) A **strong pseudorandom permutation** (or SPRP) is one which is secure against an adversary who is allowed to make queries both to the oracle and its inverse. The SPRP game is described below, while developing the notation we'll follow.

Basic Notation In an SPRP game, the adversary makes q queries, no two of them identical. For $1 \leq i \leq q$, δ^i will denote the direction of the i-th query, with $\delta^i = e$ for encryption queries and $\delta^i = d$ for decryption queries; and l^i denotes the number of blocks in the i-th query. Irrespective of δ^i, $\mathbf{p^i} = (P_1^i, ..., P_{l^i}^i)$ will denote the i-th plaintext, and $\mathbf{c^i} = (C_1^i, ..., C_{l^i}^i)$ will denote the i-th ciphertext. $\mathbf{P}$ will denote $(\mathbf{p^1}, ..., \mathbf{p^q})$ and $\mathbf{C}$ will denote $(\mathbf{c^1}, ..., \mathbf{c^q})$. $E = \{i \mid \delta^i = e\}$ denotes the set of encryption query indices, and $D = \{i \mid \delta^i = d\}$ denotes the set of decryption query indices. $q_E = \#E$ denotes the number of encryption queries, and $q_D = \#D$ denotes the number of decryption queries. (Thus, $q = q_E + q_D$.) $\sigma_E = \sum_{i \in E} l^i$ denotes the number of encryption query blocks, $\sigma_D = \sum_{i \in D} l^i$ denotes the number of decryption query blocks, and $\sigma = \sigma_E + \sigma_D = \sum_{1 \leqslant i \leqslant q} l^i$ denotes the total number of query blocks (or, equivalently, the total number of output blocks). L will denote $\max l^i$, and for $1 \leq l \leq L$, $q_l = \{i \mid l^i = l\}$ denotes the set indices corresponding to l-block queries.

Interpolation Probability For an oracle $\mathcal{O}$, given a finite set $\mathbf{Q}$ of queries and a set $\mathbf{R}$ of responses, the **interpolation probability** $\mathrm{IPr}_{\mathcal{O}}[(\mathbf{Q}, \mathbf{R})]$ is defined as $\Pr[\mathcal{O}(\mathbf{Q}) = \mathbf{R}]$, i.e., the probability that $\mathcal{O}$ takes $\mathbf{Q}$ to $\mathbf{R}$. In our setup, we'll simply write this as $\mathrm{IPr}[\mathbf{P} \to \mathbf{C}]$. (Note that $\mathbf{Q}$ may here consist of elements from both $\mathbf{P}$ and $\mathbf{C}$. The notation is just for convenience.) The interpolation probability for an ideal random permutation is given by

$$\mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}] = \prod_{1 \leqslant l \leqslant L} \frac{1}{P_{q_l}^{N^l}}.$$

The standard inequality $P_j^i \geq (1 - \frac{j^2}{i}) \cdot i^j$ will often be used to obtain bounds on the interpolation probabilities.

Coefficient H Technique $\mathbf{Q}$ and $\mathbf{R}$ together form a **view**. Suppose certain views are called **good views**, and the rest are called **bad views**, subject to the condition that an adversary cannot force a view to be bad (through his

choice of queries). Suppose that for a good view, the interpolation probability for a permutation $\mathcal{E}$ is not less than $(1-\epsilon_1)$ times the interpolation probability for an ideal random permutation. Suppose further that for an ideal random permutation, a view is good with probability not less than $(1-\epsilon_2)$. Then $\mathcal{E}$ cannot be distinguished from random with an advantage greater than $\epsilon_1+\epsilon_2$. This result is due to Jacques Patarin [5], and will be a key result in our security proofs.

The Construction The class of constructions we discuss here uses k layers of a secure Online or Online-But-Last Cipher $\mathcal{E}$ alternated with $k-1$ layers of a simple linear mixing function, like rev, to get an SPRP, with birthday security (for $k=2$, $\mathcal{E}$ secure Online-but-Last) and beyond-birthday secuirty (for $k=3$, $\mathcal{E}$ secure Online). We'll deal with these two cases separately.

3 Two Layers of Secure Online Permutation

3.1 The Original Construction

Let $\mathcal{E}$ be a secure online permutation. The construction $\Pi^2_{\mathsf{rev}}(\mathcal{E})$ originally suggested consists of two layers of $\mathcal{E}$ with a layer of rev in between. Thus, encryption is $\mathcal{E}\circ\mathsf{rev}\circ\mathcal{E}$, and decryption is $\mathcal{E}^{-1}\circ\mathsf{rev}\circ\mathcal{E}^{-1}$.

3.2 Attack

It is easy to mount a 4-query SPRP attack on this construction, as shown in Figure 3.2. We begin with a three-block encryption query with $p_1p_2p_3$ and get $c_3c_2c_1$ in response. Let $\mathcal{E}(p_1p_2p_3)$ be called $x_1x_2x_3$. Then $c_3c_2c_1=\mathcal{E}(x_3x_2x_1)$. We next make a two-block decryption query with c_3c_2, and get $p'_2p'_3$ in response. Since $\mathcal{E}$ is online, $\mathcal{E}^{-1}(c_3c_2)=x_3x_2$, so $p'_2p'_3=\mathcal{E}^{-1}(x_2x_3)$. From this we see that

$$x_2=\mathcal{E}(p'_2).$$

Our third query is a two-block encryption query with p_1p_2, yielding $c'_2c'_1$. Again, $\mathcal{E}(p_1p_2)=x_1x_2$, so $\mathcal{E}(x_2x_1)=c'_2c'_1$. From this we see that

$$\mathcal{E}(x_2)=c'_2.$$

Finally, we make a one-block encryption query with p'_2. Since, $x_2=\mathcal{E}(p'_2)$ and $\mathcal{E}(x_2)=c'_2$, this will yield c'_2, which completes the attack.

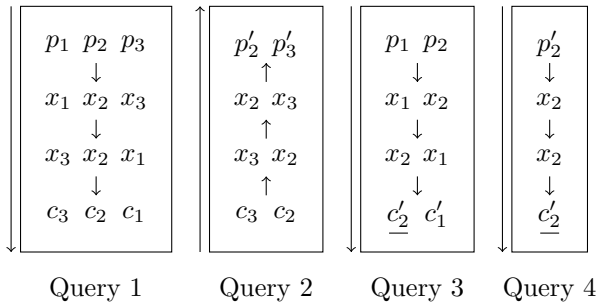

Figure 1: A 4-Query Attack

4 Two Layers of Secure Online-But-Last Permutation for Birthday Security

4.1 Setup

In the new construction $\Pi^2_{\mathsf{rev}}(\mathcal{E})$, keeping everything else the same, we let $\mathcal{E}$ be a secure online-but-last permutation. We'll show that this change is enough to grant it birthday security. For simplicity, we assume different keys are being used in the two layers of $\mathcal{E}$, and call them $\mathcal{E}_1$ and $\mathcal{E}_2$. Thus, encryption is $\mathcal{E}_2 \circ \mathsf{rev} \circ \mathcal{E}_1$, and decryption is $\mathcal{E}_1^{-1} \circ \mathsf{rev} \circ \mathcal{E}_2^{-1}$. For $1 \leq i \leq q$, $\mathcal{E}_1(\mathbf{p^i})$ will be denoted $\mathbf{x^i}$. $\mathbf{X}$ will denote $(\mathbf{x^1}, ..., \mathbf{x^q})$. For notational convenience, we'll add an extra layer of rev at the bottom. Thus, $\mathbf{c^i} = \mathcal{E}_2(\mathbf{x^{i}}^R)^R$.

4.2 Freshness and Prefixes

Here we define two important notions, that we'll need again in the next section, under slightly modified definitions.

Equivalence Query indices i and i' are called j**-encryption equivalent** for some $j < \min(l^i, l^{i'})$ if either $i = i'$, or

$$\mathbf{p^i}_{1..j} = \mathbf{p^{i'}}_{1..j}.$$

This is denoted as $i \sim_{e_j} i'$. Similarly, i and i' are called j**-decryption equivalent** for some $j < \min(l^i, l^{i'})$ if either $i = i'$, or

$$\mathbf{c^i}_{(l_i-j+1)..l_i} = \mathbf{c^{i'}}_{(l_{i'}-j+1)..l_{i'}}.$$

This is denoted as $i \sim_{d_j} i'$. Clearly, whenever $i \sim_{e_j} i'$, we have $X^i_j = X^{i'}_j$, and whenever $i \sim_{d_j} i'$, we have $X^i_{l^i-j+1} = X^{i'}_{l^{i'}-j+1}$.

Freshness and Ancestors A query index i, $1 \leq i \leq q$, is called j-**fresh**, $j \geq 1$ if $j = l^i$ and $i \in E$, or $j = 1$ and $i \in D$, or $1 < j < l^i$ and $\nexists i' \leq i$ with $j < l^{i'}$ such that $i \sim_{e_j} i'$ or $i \sim_{d_j} i'$. When i is j-fresh, X_j^i is called a fresh X block. The **encryption** j-**ancestor** of a query index i is defined as

$$A_j^e(i) = \min_{i \sim_{e_j} i'} i'.$$

Similarly, the **decryption** j-**ancestor** of a query index i is defined as

$$A_j^d(i) = \min_{i \sim_{d_j} i'} i'.$$

Prefix Matching Let $\mathcal{P}_{\mathbf{P}} = \mathcal{P}(\{\mathbf{p^i} \mid i \in E\})$, and $\mathcal{P}_{\mathbf{C}} = \mathcal{P}(\{\mathbf{c^i} \mid i \in D\})$. For $\mathbf{w} \in \mathcal{P}_{\mathbf{P}}$, let $m_{\mathbf{P}}(\mathbf{w})$ denote $\#\{x \mid \mathbf{w}x \in \mathcal{P}_{\mathbf{P}}\}$, and $m_{\mathbf{P}}^-(\mathbf{w})$ denote $\#\{x \mid \mathbf{w}x \in \mathcal{P}_{\mathbf{P}^-}\}$, where

$$\mathcal{P}_{\mathbf{P}^-} = \{\mathbf{w} \in \mathcal{P}_{\mathbf{P}} \mid \mathbf{w} \text{ does not intersect with last block of } \mathbf{p^i} \text{ for any } i \in E\}.$$

Also, $m_{\mathbf{C}}(\mathbf{w})$ will denote $\#\{x \mid \mathbf{w}x \in \mathcal{P}_{\mathbf{C}}\}$, and $m_{\mathbf{C}}^-(\mathbf{w})$ will denote $\#\{x \mid \mathbf{w}x \in \mathcal{P}_{\mathbf{C}^-}\}$, where

$$\mathcal{P}_{\mathbf{C}^-} = \{\mathbf{w} \in \mathcal{P}_{\mathbf{C}} \mid \mathbf{w} \text{ does not intersect with first block of } \mathbf{c^i} \text{ for any } i \in D\}.$$

4.3 Towards a Proof of Security

Claim We claim that the distinguishing advantage of an SPRP adversary over $\Pi_{\mathsf{rev}}^2(\mathcal{E})$ cannot exceed $\frac{3q^2}{N}$.

We now develop some apparatus required for proving this claim.

Good Views A view $\{(\delta^i)_{1 \leq i \leq q}, \mathbf{P}, \mathbf{C}\}$ is called **good** if:

- $(\forall i \in E)(\nexists i' < i)(C_{l^i}^i = C_{l^{i'}}^{i'})$,
- $(\forall i \in D)(\nexists i' < i)(P_1^i = P_1^{i'})$.

We shall show that the Interpolation Probability for a Good View under $\Pi_{\mathsf{rev}}^2(\mathcal{E})$ does not differ from that under the Ideal Random Permutation by more than a fraction of $\frac{2q^2}{N}$. From there, the claim will follow using Patarin's Technique. We first lay down some terminology, and then proceed to calculating the Interpolation Probability.

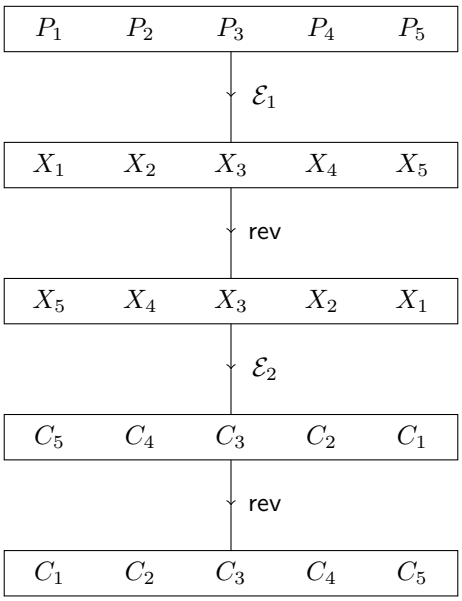

Figure 2: SPRP construction with birthday security using two layers of an online-but-last cipher $\mathcal{E}$ around one layer of rev

Variables All X_j^i's will be called **variables**. They together represent the internal state of the entire computation.

Basis All fresh X blocks together form what we call the **basis**. Assigning values to the basis variables assigns values to all variables.

Extension Chains Pick $i \in E, j \in \{1, ..., l^i\}$. Then X_j^i is a variable. Let b_1 be j, and a_1 be $A_j^e(i)$. Having obtained $b_1, ..., b_k$ and $a_1, ..., a_k$, we stop if k is odd and $a_k \in E$, or if k is even and $a_k \in D$. Otherwise, let $b_{k+1} = l^{a_k} - 1 - b_k$, and a_{k+1} be $A_{b_{k+1}}^{\delta^{a_k}}(a_k)$. Since $a_{k+1} > a_k$, this terminates after finitely many steps, say upon obtaining a_{k_0}. Then we call $((b_1, a_1), ..., (b_{k_0}, a_{k_0}))$ the **extension chain** of X_j^i.

Admissibility An assignment of values to the basis variables is called **admissible** if:

- $(\nexists i, i' \in E)(X_{l^i}^i = X_{l^{i'}}^{i'})$
- $(\nexists i, i' \in D)(X_1^i = X_1^{i'})$

- $\mathbf{p^i}$ and $\mathbf{x^i}$ are online-but-last compatible for each i
- ${\mathbf{c^i}}^R$ and ${\mathbf{x^i}}^R$ are online-but-last compatible for each i

Extending an admissible assignement Suppose we've assigned values to all basis variables, such that the assignment does not violate any of the admissiblity criteria. We'll extend it to get an admissible assignment for all variables. X_j^1 is a basis for $1 \leq j \leq l^1$. For some $i_0 > 1$, having assigned values to all X_j^i for $1 \leq i < i_0, 1 \leq j \leq l^i$, we put, for $1 \leq j \leq l^{i_0}$, $X_j^{i_0} = X_j^{A_j^e(i_0)}$ if $i_0 \in E$, and $X_{l^{i_0}-j+1}^{i_0} = X_{l^{A_j^d(i_0)}-j+1}^{A_j^d(i_0)}$ if $i_0 \in D$.

Every admissible choice of basis blocks leads to a unique assignment of values to the variables that is compatible with the given (good) view. That the assignment is unique is trivial, because the basis elements are themselves variables. To see that the assignment is compatible with the given view, we just note that every variable takes the value of a unique basis variable, that can be located by tracing back along the extension chain till we stop. Instead of talking of an admissible assignment for basis variables, we'll simply talk instead of an admissible $\mathbf{X}$.

4.4 The Proof

Interpolation Probability We shall show in the next section that

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq \frac{(1-\epsilon_1)}{N^\sigma},$$

where $\epsilon_1 = \frac{q^2}{N}$.

Ideal Random Permutation The interpolation probability for an ideal random permutation is given by

$$\begin{aligned}
\mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}] &= \prod_{1 \leqslant l \leqslant L} \frac{1}{P_{q_l}^{N^l}} \\
&\leq \prod_{1 \leqslant l \leqslant L} \frac{1}{(1-\frac{q_l^2}{N^l}) \cdot N^{lq_l}} \\
&\leq \frac{1}{N^\sigma} \cdot \frac{1}{1 - \sum\limits_{1 \leqslant l \leqslant L} \frac{q_l^2}{N^l}} \\
&\leq \frac{1}{N^\sigma} \cdot \frac{1}{1-\epsilon_1},
\end{aligned}$$

since $q = \sum_{1 \leqslant l \leqslant L} q_l$.

Thus,

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq (1 - 2\epsilon_1) \cdot \mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}].$$

Applying Patarin's Technique Let ϵ_2 denote the probability of a view being bad under an ideal random permutation. Then

$$\epsilon_2 \leq \sum_{1 \leqslant i \leqslant q} \frac{i}{N} \leq \epsilon_1.$$

Thus, by Patarin's Technique, we can conclude that the distinguishing advantage cannot exceed $\frac{3q^2}{N}$, as claimed.

4.5 Calculating the Interpolation Probability

Counting Admissible Assignments Let $\mathcal{A} = \{\mathbf{X} \mid \mathbf{X} \text{ is admissible}\}$. We want to count $\#\mathcal{A}$. The blocks $\{X^i_{l^i}\}_{i \in E}$, $\{X^i_1\}_{i \in D}$ can be chosen in $P^N_{q_E} \cdot P^N_{q_D}$ ways. The remaining blocks can be chosen in $(\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})}) \cdot (\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})})$ ways. Thus,

$$\#\mathcal{A} = P^N_{q_E} \cdot P^N_{q_D} \cdot (\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})}) \cdot (\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})}).$$

A Bound on the Total Number of Possible Assignments Recalling that $\mathcal{E}_1$ and $\mathcal{E}_2$ are online-but-last, the total number of choices for $\mathbf{X}$ cannot exceed $(\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})}) \cdot N^{\sigma_E} \cdot (\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})}) \cdot N^{\sigma_D} \cdot N^q$.

Interpolation Probability

$$\begin{aligned}
\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] &\geq \sum_{\mathbf{X} \in \mathcal{A}} \Pr[\mathcal{E}_1(\mathbf{P}) = \mathbf{X}] \cdot \Pr[\mathcal{E}_2(\mathsf{rev}(\mathbf{X})) = \mathsf{rev}(\mathbf{C})] \\
&\geq \frac{\#\mathcal{A}}{(\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})}) \cdot N^{\sigma_E} \cdot (\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})}) \cdot N^{\sigma_D} \cdot N^q} \\
&= \frac{P^N_{q_E} \cdot P^N_{q_E}}{N^q} \cdot \frac{1}{N^\sigma} \\
&\geq \frac{(1 - \frac{q_E^2}{N}) \cdot N^{q_E} \cdot (1 - \frac{q_E^2}{N}) \cdot N^{q_E}}{N^q} \cdot \frac{1}{N^\sigma} \\
&\geq \frac{(1 - \epsilon_1)}{N^\sigma}
\end{aligned}$$

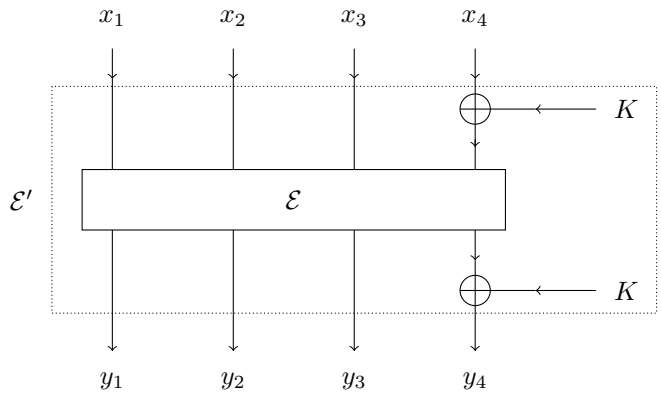

Figure 3: Getting online-but-last from online

as claimed in the previous section, which completes the proof.

4.6 Obtaining an Online-but-Last Cipher from an Online Cipher

We now state an easy way of getting an Online-but-last Cipher from an Online Cipher. Suppose $\mathcal{E}$ is a secure Online cipher, and let $+_K$ represent the function that adds K to the last block of the input. Then $\mathcal{E}'(K,.) = +_K \circ \mathcal{E} \circ +_K$ is a secure Online-but-last Cipher, with an extra key K. This is illustrated in Figure 4.6.

This construction is Online-but-last secure because, for any plaintext with l blocks, the first $l-1$ blocks are simply encrypted through $\mathcal{E}$, and thus behave like they come from an ideal random Online permutation, as required, and since K is chosen randomly, the last block of the output is uniform. Thus, the output behaves like it comes from an ideal random Online-but-last permutation.

5 Three Layers of Secure Online Permutation for Beyond-Birthday Security

5.1 Setup

Let $\mathcal{E}$ now be a secure online permutation. The construction $\Pi^3_{\mathsf{rev}}(\mathcal{E})$ consists of three layers of $\mathcal{E}$ with two layers of rev in between. Again, for simplicity, we assume different keys are being used in the three layers of $\mathcal{E}$, and call them

$\mathcal{E}_1$, $\mathcal{E}_2$ and $\mathcal{E}_3$. Thus, encryption is $\mathcal{E}_3 \circ \mathsf{rev} \circ \mathcal{E}_2 \circ \mathsf{rev} \circ \mathcal{E}_1$, and decryption is $\mathcal{E}_1^{-1} \circ \mathsf{rev} \circ \mathcal{E}_2^{-1} \circ \mathsf{rev} \circ \mathcal{E}_3^{-1}$. For $1 \leq i \leq q$, $\mathcal{E}_1(\mathbf{p^i})$ will be denoted $\mathbf{x^i}$, and $\mathcal{E}_3^{-1}(\mathbf{c^i})$ will be denoted $\mathbf{y^i}$. (Thus, $\mathcal{E}_2(\mathbf{x}^{iR}) = \mathbf{y}^{iR}$.) $\mathbf{X}$ will denote $(\mathbf{x^1}, ..., \mathbf{x^q})$, and $\mathbf{Y}$ will denote $(\mathbf{y^1}, ..., \mathbf{y^q})$.

5.2 Freshness and Prefixes Revisited

We come back to these two notions we defined earlier, and now give them slightly modified definitions, as suited to this problem.

Equivalence The definition of j-**encryption equivalence** remains the same as before. However, i and i' will now be called j-**decryption equivalent** for some $j < \min(l^i, l^{i'})$ if either $i = i'$, or

$$\mathbf{c^i}_{1..j} = \mathbf{c^{i'}}_{1..j}.$$

Whenever $i \sim_{e_j} i'$, we still have $X_j^i = X_j^{i'}$, and whenever $i \sim_{d_j} i'$, we now have $Y_j^i = Y_j^{i'}$. j-**freshness** and j-**ancestors** are now defined as before, using our new definitions of equivalence instead of the old ones.

Prefix Matching We now let $\mathcal{P}_\mathbf{P}$ denote simply, $\mathcal{P}(\{\mathbf{p^i} \mid 1 \leq i \leq q\})$, and $\mathcal{P}_\mathbf{C}$ denote $\mathcal{P}(\{\mathbf{c^i} \mid 1 \leq i \leq q\})$. Further, while $\mathbf{w} \in \mathcal{P}_\mathbf{P}$, $m_\mathbf{P}(\mathbf{w})$ continues to denote $\#\{x \mid \mathbf{w}x \in \mathcal{P}_\mathbf{P}\}$, $m_\mathbf{P}^-(\mathbf{w})$ now stands for $\#\{x \mid \mathbf{w}x \in \mathcal{P}_{\mathbf{P}^-}\}$, where

$$\mathcal{P}_{\mathbf{P}^-} = \{\mathbf{w} \in \mathcal{P}_\mathbf{P} \mid \mathbf{w} \text{ does not intersect with the last two block of any } \mathbf{p^i}\}.$$

Similarly, $m_\mathbf{C}(\mathbf{w})$ still denotes $\#\{x \mid \mathbf{w}x \in \mathcal{P}_\mathbf{C}\}$, but $m_\mathbf{C}^-(\mathbf{w})$ now stands for $\#\{x \mid \mathbf{w}x \in \mathcal{P}_{\mathbf{C}^-}\}$, where

$$\mathcal{P}_{\mathbf{C}^-} = \{\mathbf{w} \in \mathcal{P}_\mathbf{C} \mid \mathbf{w} \text{ does not intersect with the last two blocks of any } \mathbf{c^i}\}.$$

5.3 Congruences and Partitions

A congruence $\sim$ on the set $\{1, ..., q\}$ with exactly k congruence classes, $1 \leq k \leq q$, is called a k-**partition**. (When we write k in the calculations, the $\sim$ it refers to will be clear from the context.) Let $n_1[\sim], ..., n_k[\sim]$ denote the sizes of the partitions in decreasing order. Let Π_k denote the set of all k-partitions, with $\Pi = \cup_k \Pi_k$. Let $S[\sim]$ denote the set of q-block sequences compatible with the $\sim$, i.e., whenever $\mathbf{w} \in S[\sim]$, $(\mathbf{w}_j = \mathbf{w}_{j'}) \longleftrightarrow (j \sim j')$.

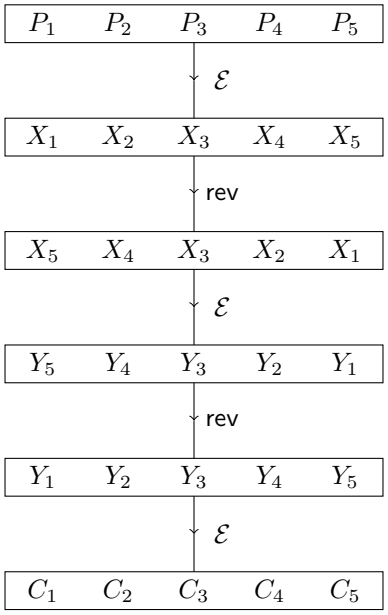

Figure 4: SPRP construction with beyond-birthday security using three layers of an online cipher $\mathcal{E}$ around two layers of rev

5.4 Towards a Proof of Security

Claim We claim that the distinguishing advantage of an SPRP adversary over $\Pi^3_{\mathsf{rev}}(\mathcal{E})$ cannot exceed $\frac{2q^2}{N^2}$.

We shall, as before, develop some apparatus for the proof. The notions introduced will be mostly ones that were also used, under slightly different definitions, in the previous proof. (Note that, for this proof, we do not need to classify any view as bad, thus eliminating the second term in Patarin's result.)

Variables $\{X^i_j, Y^i_j, 1 \leq i \leq q, 1 \leq j \leq l^i\}$ will be the variables here.

Basis We now construct the basis B. For $i \in E$:

- $X^i_j \in B$ if i is j-fresh
- $Y^i_1 \in B$ if $(\forall i' < i)(C^i_1 \neq C^{i'}_1)$
- $Y^i_j \in B, 2 \leq j \leq l^i$

For $i \in D$:

- $Y_j^i \in B$ if i is j-fresh
- $X_1^i \in B$ if $(\forall i' < i)(P_1^i \neq P_1^{i'})$
- $X_j^i \in B, 2 \leq j \leq l^i$

Extension For $i \in E$, if $Y_1^i \notin B$, find first occurrence C_1^i, i.e., smallest i' with $C_1^i = C_1^{i'}$. Then $Y_1^i = Y_1^{i'}$, and $Y_1^{i'} \in B$. If $X_j^i \notin B$, find $i' = A_\epsilon^j(i)$. Then $X_j^i = X_j^{i'}$, and $X_j^{i'} \in B$. Similarly for $i \in D$.

Admissibility We call an assignment of values to the variables admissible if it satisfies the following criteria:

- For $i \neq i'$, $(X_{l^i-1}^i, X_{l^i}^i) \neq (X_{l^{i'}-1}^{i'}, X_{l^{i'}}^{i'})$
- For $i \neq i'$, $(Y_{l^i-1}^i, Y_{l^i}^i) \neq (Y_{l^{i'}-1}^{i'}, Y_{l^{i'}}^{i'})$
- For $i \neq i'$, $X_{l^i}^i = X_{l^{i'}}^{i'}$ if and only if $Y_{l^i}^i = Y_{l^{i'}}^{i'}$
- $\mathbf{p^i}$ and $\mathbf{x^i}$ are online-but-last compatible for each i
- $\mathbf{c^i}$ and $\mathbf{y^i}$ are online-but-last compatible for each i

5.5 The Proof

Interpolation Probability We shall show that

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq (1-\epsilon) \cdot \frac{1}{P_{q-\overline{q}}^N} \cdot \frac{1}{N^{\sigma-(q-\overline{q})}},$$

where $\epsilon = \frac{\overline{q}^2}{N^2}$.

Ideal Random Permutation Now,

$$\begin{aligned}\mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}] &= \prod_{1 \leqslant l \leqslant L} \frac{1}{P_{q_l}^{N^l}} \\ &\leq \frac{1}{P_{q_1}^N} \cdot \prod_{2 \leqslant l \leqslant L} \frac{1}{(1 - \frac{q_l^2}{N^l}) \cdot N^{lq_l}} \\ &\leq \frac{1}{P_{q_1}^N} \cdot \frac{1}{N^{\sigma - q_1}} \cdot \frac{1}{1 - \sum\limits_{2 \leqslant l \leqslant L} \frac{q_l^2}{N^l}} \\ &\leq \frac{1}{P_{q_1}^N} \cdot \frac{1}{N^{\sigma - q_1}} \cdot \frac{1}{1 - \frac{(q-q_1)^2}{N^2}}.\end{aligned}$$

Putting $q_1 = q - \overline{q}$, we have

$$\mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}] \leq \frac{1}{P_{q-\overline{q}}^N} \cdot \frac{1}{N^{\sigma-(q-\overline{q})}} \cdot \frac{1}{1-\epsilon}.$$

Applying Patarin's Technique We conclude that

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq (1 - 2\epsilon) \cdot \mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}],$$

from which Patarin's Result tells us that the distinguishing advantage cannot exceed $\frac{2\overline{q}^2}{N^2}$.

5.6 Calculating the Interpolation Probability

Interpolation Probability in terms of Prefix Match counts We initially assume $l^i \geq 2, 1 \leq i \leq q$, and later incorporate the case where single block queries are allowed. We'll show that

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq P_q^{N^2} \cdot N^{2q} \cdot \frac{\prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P_{m_\mathbf{P}^-(\mathbf{w})}^N \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P_{m_\mathbf{C}^-(\mathbf{w})}^N}{\prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P_{m_\mathbf{P}(\mathbf{w})}^N \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P_{m_\mathbf{C}(\mathbf{w})}^N} \cdot \frac{1}{N^\sigma}.$$

Counting Admissible Assignments We shall count the number of admissible $(\mathbf{X}, \mathbf{Y})$ pairs. We begin with the last blocks, for which we have an equality restriction, and the last-but-one blocks. Let $\mathsf{last}(\mathbf{X})$ denote the column $\{X_{l^i}^i\}_{1 \leq i \leq q}$, and $\mathsf{lbo}(\mathbf{X})$ denote the column $\{X_{l^i-1}^i\}_{1 \leq i \leq q}$. Similarly, let $\mathsf{last}(\mathbf{Y})$ denote the column $\{Y_{l^i}^i\}_{1 \leq i \leq q}$, and $\mathsf{lbo}(\mathbf{Y})$ denote the column $\{Y_{l^i-1}^i\}_{1 \leq i \leq q}$.

The Last Blocks Fix $\sim$. Clearly,

$$\#S[\sim] = P_k^n,$$

since $\sim$ allows only k distinct values. Thus,

$$\#\{(\mathsf{last}(\mathbf{X}), \mathsf{last}(\mathbf{Y})) \mid \mathsf{last}(\mathbf{X}) \in S[\sim], \mathsf{last}(\mathbf{Y}) \in S[\sim]\} = (P_k^N)^2.$$

Now, by the admissibility criteria, whenever $X^i_{l^i} = X^{i'}_{l^{i'}}$, i.e., whenever $i \sim i'$, we need $X^i_{l^i-1} \neq X^{i'}_{l^{i'}-1}$, and similarly for $\mathbf{Y}$. Thus, given a valid choice of $(\mathsf{last}(\mathbf{X}), \mathsf{last}(\mathbf{Y}))$, we have

$$\#\{\text{valid } (\mathsf{lbo}(\mathbf{X}), \mathsf{lbo}(\mathbf{Y}))\} = (\prod_{i=1}^{k} P^N_{n_i[\sim]})^2.$$

Thus, the total number of valid choices for the last two blocks of $\mathbf{X}$ and $\mathbf{Y}$ is $(P_k^N \cdot \prod_{i=1}^k P^N_{n_i[\sim]})^2$.

The Remaining Blocks The remaining blocks need to be chosen so as to maintain online compatibility with $\mathbf{P}$ and $\mathbf{C}$. Let $T[\sim]$ denote the set $\{(\mathbf{X}, \mathbf{Y}) \text{ admissible} \mid \mathsf{last}(\mathbf{X}) \in S[\sim], \mathsf{last}(\mathbf{Y}) \in S[\sim]\}$. Then

$$\#T[\sim] = (\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m_\mathbf{P}(\mathbf{w})}) \cdot (\prod_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m_\mathbf{C}(\mathbf{w})}) \cdot (P_k^N \cdot \prod_{i=1}^{k} P^N_{n_i[\sim]})^2.$$

We note here that

$$\sum_{\sim \in \Pi} (P_k^N \cdot \prod_{i=1}^{k} P^N_{n_i[\sim]}) = P_q^{N^2}.$$

Interpolation probability Next we obtain an expression for the interpolation probability.

$$
\begin{aligned}
&\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \\
\geq &\sum_{\sim \in \Pi} \sum_{(\mathbf{X},\mathbf{Y}) \in T[\sim]} \Pr[\mathcal{E}(\mathbf{P}) = \mathbf{X}] \cdot \Pr[\mathcal{E}(\mathsf{rev}(\mathbf{X})) = \mathsf{rev}(\mathbf{Y})] \cdot \Pr[\mathcal{E}(\mathbf{Y}) = \mathbf{C}] \\
= &\sum_{\sim \in \Pi} \sum_{(\mathbf{X},\mathbf{Y}) \in T[\sim]} \frac{1}{\prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{P}}} P^N_{m_{\mathbf{P}}(\mathbf{w})}} \cdot \Big(\frac{1}{N^{\sigma-2q}} \cdot \frac{1}{P^N_k} \cdot \frac{1}{\prod\limits_{i=1}^{k} P^N_{n_i[\sim]}}\Big) \cdot \frac{1}{\prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{C}}} P^N_{m_{\mathbf{C}}(\mathbf{w})}} \\
= &\frac{1}{\prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{P}}} P^N_{m_{\mathbf{P}}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{C}}} P^N_{m_{\mathbf{C}}(\mathbf{w})}} \cdot \frac{1}{N^{\sigma-2q}} \cdot \sum_{\sim \in \Pi} \sum_{(\mathbf{X},\mathbf{Y}) \in T[\sim]} \frac{1}{P^N_k \cdot \prod\limits_{i=1}^{k} P^N_{n_i[\sim]}} \\
= &\frac{1}{\prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{P}}} P^N_{m_{\mathbf{P}}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{C}}} P^N_{m_{\mathbf{C}}(\mathbf{w})}} \cdot \frac{1}{N^{\sigma-2q}} \cdot \\
&\sum_{\sim \in \Pi} \frac{\prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{P}}} P^N_{m^-_{\mathbf{P}}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{C}}} P^N_{m^-_{\mathbf{C}}(\mathbf{w})} \cdot (P^N_k \cdot \prod_{i=1}^{k} P^N_{n_i[\sim]})^2}{P^N_k \cdot \prod\limits_{i=1}^{k} P^N_{n_i[\sim]}} \\
= &P_q^{N^2} \cdot N^{2q} \cdot \frac{\prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{P}}} P^N_{m^-_{\mathbf{P}}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{C}}} P^N_{m^-_{\mathbf{C}}(\mathbf{w})}}{\prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{P}}} P^N_{m_{\mathbf{P}}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{C}}} P^N_{m_{\mathbf{C}}(\mathbf{w})}} \cdot \frac{1}{N^{\sigma}},
\end{aligned}
$$

as claimed before.

Allowing Single-Block Queries The above analysis assumes all queries to have two or more blocks. Now we analyse the case when single-block queries are allowed. The counting for the last blocks remains the same, except that the single-block queries must correspond to distinct last blocks in the equivalence relation. The counting for the last-but-one blocks, however, need to be adjusted to accommodate the single-block queries. We shall show that

$$
\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq P_{\overline{q}}^{N^2} \cdot P^N_{q-\overline{q}} \cdot N^{q+\overline{q}} \cdot \frac{\prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{P}}} P^N_{m^-_{\mathbf{P}}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{C}}} P^N_{m^-_{\mathbf{C}}(\mathbf{w})}}{\prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{P}}} P^N_{m_{\mathbf{P}}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_{\mathbf{C}}} P^N_{m_{\mathbf{C}}(\mathbf{w})}} \cdot \frac{1}{N^{\sigma}}.
$$

Fixing the Counts Suppose $\mathbf{1} \subset \{1, ..., q\}$ is the set of all single-block query indices. We now fix a $\sim$ as before, with the additional restriction that $\sim$ puts the indices in $\mathbf{1}$ into distinct classes. (We call the collection of equivalence relations satisfying this new criterion $\Pi*$.) Let $\pi_1[\sim], ..., \pi_k[\sim]$ denote the partitions of $\sim$ arranged in order of decreasing size. (Thus, for $1 \leq i \leq k$, $n_i[\sim] = \#\pi_i[\sim]$.) We define $\overline{n}_i = \#(\pi_i[\sim] \setminus \mathbf{1})$. Thus, $\overline{n}_i[\sim]$ counts the number of indices in $\pi_i[\sim]$ that

correspond to indices of length two or more. (Note that $\overline{n}_1[\sim], ..., \overline{n}_k[\sim]$ need not be in decreasing order. But that will not bother us.)

In counting the last-but-one blocks, we'll now simply ignore the single-block queries, and count for the rest. The modified expression is thus

$$\#T[\sim] = (\prod_{\mathbf{w}\in\mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})}) \cdot (\prod_{\mathbf{w}\in\mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})}) \cdot (P^N_k \cdot \prod_{i=1}^{k} P^N_{\overline{n}_i[\sim]})^2.$$

Let $\overline{q}$ denote $q - \#\mathbf{1}$, the number of queries with two or more blocks. Then the new expression for $\Pr[\mathcal{E}(\mathsf{rev}(\mathbf{X})) = \mathsf{rev}(\mathbf{Y})]$ in our calculation of $\mathrm{IPr}[\mathbf{P} \to \mathbf{C}]$ becomes

$$\frac{1}{N^{\sigma-(q+\overline{q})}} \cdot \frac{1}{P^N_k} \cdot \frac{1}{\prod_{i=1}^{k} P^N_{\overline{n}_i[\sim]}}.$$

Putting it back in the Earlier Expression We note next that

$$\sum_{\sim\in\Pi*} (P^N_k \cdot \prod_{i=1}^{k} P^N_{\overline{n}_i[\sim]}) = P^{N^2}_{\overline{q}} \cdot P^N_{q-\overline{q}},$$

and putting this in our earlier calculation gives

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq P^{N^2}_{\overline{q}} \cdot P^N_{q-\overline{q}} \cdot N^{q+\overline{q}} \cdot \frac{\prod_{\mathbf{w}\in\mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})} \cdot \prod_{\mathbf{w}\in\mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})}}{\prod_{\mathbf{w}\in\mathcal{P}_\mathbf{P}} P^N_{m_\mathbf{P}(\mathbf{w})} \cdot \prod_{\mathbf{w}\in\mathcal{P}_\mathbf{C}} P^N_{m_\mathbf{C}(\mathbf{w})}} \cdot \frac{1}{N^\sigma},$$

as claimed.

Simplifying the Inequality We shall show next that

$$\frac{\prod_{\mathbf{w}\in\mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})} \cdot \prod_{\mathbf{w}\in\mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})}}{\prod_{\mathbf{w}\in\mathcal{P}_\mathbf{P}} P^N_{m_\mathbf{P}(\mathbf{w})} \cdot \prod_{\mathbf{w}\in\mathcal{P}_\mathbf{C}} P^N_{m_\mathbf{C}(\mathbf{w})}} \geq \frac{1}{(P^N_{q-\overline{q}})^2} \cdot \frac{1}{N^{4\overline{q}}}.$$

We begin by analysing the prefix-match counts. Now,

$$\frac{P^N_{m^-_\mathbf{P}(\mathbf{w})}}{P^N_{m_\mathbf{P}(\mathbf{w})}} = \frac{1}{P^{N-m^-_\mathbf{P}(\mathbf{w})}_{m_\mathbf{P}(\mathbf{w})-m^-_\mathbf{P}(\mathbf{w})}} \geq \frac{1}{N^{m_\mathbf{P}(\mathbf{w})-m^-_\mathbf{P}(\mathbf{w})}}.$$

and similarly for $\frac{P^N_{m^-_{\mathbf{C}}(\mathbf{w})}}{P^N_{m_{\mathbf{C}}(\mathbf{w})}}$. It is easy to see that

$$\sum_{\mathbf{w}\in\mathcal{P}_{\mathbf{P}}} (m_{\mathbf{P}}(\mathbf{w}) - m^-_{\mathbf{P}}(\mathbf{w})) = \#(\mathcal{P}_{\mathbf{P}} \setminus \mathcal{P}_{\mathbf{P}^-}),$$
$$\sum_{\mathbf{w}\in\mathcal{P}_{\mathbf{C}}} (m_{\mathbf{C}}(\mathbf{w}) - m^-_{\mathbf{C}}(\mathbf{w})) = \#(\mathcal{P}_{\mathbf{C}} \setminus \mathcal{P}_{\mathbf{C}^-}).$$

By construction of the sets $\mathcal{P}_{\mathbf{P}}$ and $\mathcal{P}_{\mathbf{P}^-}$, each element of $\mathcal{P}_{\mathbf{P}} \setminus \mathcal{P}_{\mathbf{P}^-}$ must correspond to a distinct x such that x is one of the last two blocks of $\mathbf{p}^{\mathbf{i}}$ for some i. Thus, $\#(\mathcal{P}_{\mathbf{P}} \setminus \mathcal{P}_{\mathbf{P}^-}) \leq q + \overline{q}$, and similarly $\#(\mathcal{P}_{\mathbf{C}} \setminus \mathcal{P}_{\mathbf{C}^-}) \leq q + \overline{q}$.

Let λ be the empty word. For each $i \in \mathbf{1}$, $X^i_{l^i} = X^i_1$ is in $\mathcal{P}_{\mathbf{P}}$ but not in $\mathcal{P}_{\mathbf{P}^-}$. Thus, $m_{\mathbf{P}}(\lambda) - m^-_{\mathbf{P}}(\lambda) \geq q - \overline{q}$, and similarly $m_{\mathbf{C}}(\lambda) - m^-_{\mathbf{C}}(\lambda) \geq q - \overline{q}$. Let $a_{\mathbf{P}} = m_{\mathbf{P}}(\lambda) - m^-_{\mathbf{P}}(\lambda) - (q - \overline{q})$, and $a_{\mathbf{C}} = m_{\mathbf{C}}(\lambda) - m^-_{\mathbf{C}}(\lambda) - (q - \overline{q})$. So,

$$\sum_{\mathbf{w}\in\mathcal{P}_{\mathbf{P}},\mathbf{w}\neq\lambda} (m_{\mathbf{P}}(\mathbf{w}) - m^-_{\mathbf{P}}(\mathbf{w})) \leq 2\overline{q} - a_{\mathbf{P}},$$
$$\sum_{\mathbf{w}\in\mathcal{P}_{\mathbf{C}},\mathbf{w}\neq\lambda} (m_{\mathbf{C}}(\mathbf{w}) - m^-_{\mathbf{C}}(\mathbf{w})) \leq 2\overline{q} - a_{\mathbf{C}}.$$

From this we conclude that

$$\frac{\prod_{\mathbf{w}\in\mathcal{P}_{\mathbf{P}}} P^N_{m^-_{\mathbf{P}}(\mathbf{w})} \cdot \prod_{\mathbf{w}\in\mathcal{P}_{\mathbf{C}}} P^N_{m^-_{\mathbf{C}}(\mathbf{w})}}{\prod_{\mathbf{w}\in\mathcal{P}_{\mathbf{P}}} P^N_{m_{\mathbf{P}}(\mathbf{w})} \cdot \prod_{\mathbf{w}\in\mathcal{P}_{\mathbf{C}}} P^N_{m_{\mathbf{C}}(\mathbf{w})}} \geq \frac{1}{(P^N_{q-\overline{q}})^2} \cdot \frac{1}{N^{4\overline{q}-a_{\mathbf{P}}-a_{\mathbf{C}}}} \geq \frac{1}{(P^N_{q-\overline{q}})^2} \cdot \frac{1}{N^{4\overline{q}}},$$

as claimed.

The Final Expression Putting all this together, we have

$$\begin{aligned}\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] &\geq \frac{P^{N^2}_{\overline{q}}}{P^N_{q-\overline{q}}} \cdot \frac{1}{N^{3\overline{q}-q}} \cdot \frac{1}{N^{\sigma}} \\ &\geq (1-\epsilon) \cdot \frac{1}{P^N_{q-\overline{q}}} \cdot \frac{1}{N^{\sigma-(q-\overline{q})}},\end{aligned}$$

which completes the proof.

5.7 Improved Security for Queries of Size at least $2m$

When all the queries are guaranteed to be at least $2m$ blocks long, for some $m \geq 1$, we can improve this security bound.

Claim When each query is guaranteed to have at least $2m$ blocks, the distinguishing advantage of an SPRP adversary over $\Pi^3_{\mathsf{rev}}(\mathcal{E})$ cannot exceed $\frac{2q^2}{N^{2m}}$.

Proof of Claim We'll show below that

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq \frac{1-\epsilon}{N^\sigma},$$

where $\epsilon = \frac{q^2}{N^{2m}}$.

We recall that

$$\mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}] = \prod_{1 \leqslant l \leqslant L} \frac{1}{P^{N^l}_{q_l}}.$$

From this we get

$$\begin{aligned}\mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}] &\leq \prod_{1 \leqslant l \leqslant L} \frac{1}{(1-\frac{q_l^2}{N^l}) \cdot N^{lq_l}} \\ &\leq \frac{1}{N^\sigma} \cdot \frac{1}{1 - \sum\limits_{1 \leqslant l \leqslant L} \frac{q_l^2}{N^l}}.\end{aligned}$$

Now, $N^l \geq N^{2m}$ for each l, and $\sum_{1 \leqslant l \leqslant L} q_l^2 \leq q^2$. Thus,

$$\mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}] \leq \frac{1}{N^\sigma} \cdot \frac{1}{1-\epsilon}.$$

As before, we conclude that

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq (1-2\epsilon) \cdot \mathrm{IPr}^*[\mathbf{P} \to \mathbf{C}],$$

from which Patarin's Result tells us that the distinguishing advantage cannot exceed $\frac{2q^2}{N^{2m}}$.

Calculating the Interpolation Probability We'll begin by showing that

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq P_q^{N^{2m}} \cdot N^{2mq} \cdot \frac{\prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})}}{\prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m_\mathbf{P}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m_\mathbf{C}(\mathbf{w})}} \cdot \frac{1}{N^\sigma}.$$

Arguing as before, $\#(\mathcal{P}_\mathbf{P} \setminus \mathcal{P}_{\mathbf{P}^-}) \leq 2mq$, and $\#(\mathcal{P}_\mathbf{C} \setminus \mathcal{P}_{\mathbf{C}^-}) \leq 2mq$. Thus,

$$\frac{\prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})}}{\prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m_\mathbf{P}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m_\mathbf{C}(\mathbf{w})}} \geq \frac{1}{N^{4mq}}.$$

Putting all this together, we have

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq \frac{P_q^{N^{2m}}}{N^{2mq}} \cdot \frac{1}{N^{\sigma}} \geq \frac{1-\epsilon}{N^{\sigma}},$$

where $\epsilon = \frac{q^2}{N^{2m}}$.

Counting Admissible Assignments As before, we bound the Interpolation Probability by counting the number of admissible assignments. Now, instead of counting the last two blocks separately, we count the last $2m$ blocks separately.

Last $2m$ Blocks Let $\sim$ now denote an equivalence relation over the last $2m-1$ blocks, i.e., on the set $\{1, ..., q\}^{2m-1}$, with $k, n_1[\sim], ..., n_k[\sim]$ defined as before. Clearly, the number of valid choices for the last $2m$ blocks of $\mathbf{X}$ and $\mathbf{Y}$ is $(P_k^{N^{2m-1}} \cdot \prod_{i=1}^{k} P^N_{n_i[\sim]})^2$.

The Remaining Blocks For $\mathbf{w} \in \mathcal{P}_{\mathbf{P}}$, let $m^-_{\mathbf{P}}(\mathbf{w})$ now denote $\#\{x | \mathbf{w}x \in \mathcal{P}_{\mathbf{P}^-}\}$, where

$$\mathcal{P}_{\mathbf{P}^-} = \{\mathbf{w} \in \mathcal{P}_{\mathbf{P}} | \mathbf{w} \text{ does not intersect with last } 2m \text{ blocks of } \mathbf{p}^{\mathbf{i}} \text{ for any } i\},$$

with $m^-_{\mathbf{C}}(\mathbf{w})$ similarly defined.

Let $T[\sim]$ now denote the set $\{(\mathbf{X}, \mathbf{Y}) \text{ admissible} \mid \text{last } 2m-1 \text{ blocks of } \mathbf{X} \in S[\sim], \text{ last } 2m-1 \text{ blocks of } \mathbf{Y} \in S[\sim]\}$. Then

$$\#T[\sim] = (\prod_{\mathbf{w} \in \mathcal{P}_{\mathbf{P}}} P^N_{m^-_{\mathbf{P}}(\mathbf{w})}) \cdot (\prod_{\mathbf{w} \in \mathcal{P}_{\mathbf{C}}} P^N_{m^-_{\mathbf{C}}(\mathbf{w})}) \cdot (P_k^{N^{2m-1}} \cdot \prod_{i=1}^{k} P^N_{n_i[\sim]})^2.$$

Also,

$$\sum_{\sim \in \Pi} (P_k^{N^{2m-1}} \cdot \prod_{i=1}^{k} P^N_{n_i[\sim]}) = P_q^{N^{2m}}.$$

Interpolation Probability The new expression for $\Pr[\mathcal{E}(\mathsf{rev}(\mathbf{X})) = \mathsf{rev}(\mathbf{Y})]$ in our calculation of $\mathrm{IPr}[\mathbf{P} \to \mathbf{C}]$ becomes

$$\frac{1}{N^{\sigma-2mq}} \cdot \frac{1}{P_k^{N^{2m-1}}} \cdot \frac{1}{\prod_{i=1}^{k} P^N_{n_i[\sim]}}.$$

Substituting the expression for $\#T[\sim]$ above and summing over $\sim$, we have

$$\mathrm{IPr}[\mathbf{P} \to \mathbf{C}] \geq P_q^{N^{2m}} \cdot N^{2mq} \cdot \frac{\prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m^-_\mathbf{P}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m^-_\mathbf{C}(\mathbf{w})}}{\prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{P}} P^N_{m_\mathbf{P}(\mathbf{w})} \cdot \prod\limits_{\mathbf{w} \in \mathcal{P}_\mathbf{C}} P^N_{m_\mathbf{C}(\mathbf{w})}} \cdot \frac{1}{N^\sigma},$$

which completes the proof.

6 Conclusion

In conclusion, we recall that while three passes of a secure online cipher interleaved with a simple mixing layer ensures beyond-birthday SPRP security, two passes with a reverse in between falls short of SPRP security. This can be fixed by a slight compromise in the efficiency of the secure online cipher, by replacing it with a secure online-but-last cipher. We also note the importance of simple and transparent security proofs, and the usefulness of Patarin's Technique in achieving this.

References

[1] Elena Andreeva, Guy Barwell, Dan Page, and Martijn Stam. Turning online ciphers off. Cryptology ePrint Archive, Report 2015/485, 2015. `http://eprint.iacr.org/`.

[2] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. Parallelizable and authenticated online ciphers. Cryptology ePrint Archive, Report 2013/790, 2013. `http://eprint.iacr.org/`.

[3] O. Goldreich. *Foundations of Cryptography: Fragments of a Book*. Weizmann Institute of Science, 1995.

[4] Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 482–499. Springer Berlin Heidelberg, 2003.

[5] Jacques Patarin. The coefficients h technique. In RobertoMaria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer Berlin Heidelberg, 2009.

[6] Phillip Rogaway and Haibin Zhang. Online ciphers from tweakable blockciphers. In Aggelos Kiayias, editor, *Topics in Cryptology CT-RSA 2011*,

volume 6558 of *Lecture Notes in Computer Science*, pages 237–249. Springer Berlin Heidelberg, 2011.

[7] Data Encryption Standard. Fips pub 46. *Appendix A, Federal Information Processing Standards Publication*, 1977.