Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes

Virgil D. Gligor* Pompiliu Donescu

VDG Inc
6009 Brookside Drive
Chevy Chase, Maryland 20815
{gligor, pompiliu}@eng.umd.edu

August 18, 2000

Abstract

We present the eXtended Ciphertext Block Chaining (XCBC) schemes or modes of encryption that can detect encrypted-message forgeries with high probability even when used with typical non-cryptographic Manipulation Detection Code (MDC) functions (e.g., bitwise exclusive-or and cyclic redundancy code (CRC) functions). These modes detect encrypted-message forgeries at low cost in performance, power, and implementation, and preserve both message secrecy and integrity in a single pass over the message data. Their performance and security scale directly with those of the underlying block encryption function. We also present the XECB message authentication modes. These modes have all the operational properties of the XOR-MAC modes (e.g., fully parallel and pipelined operation, incremental updates, and out-of-order verification), and have better performance. They are intended for use either stand-alone or with encryption modes that have similar properties (e.g., counter-based XOR encryption). However, the XECB-MAC modes have higher upper bounds on the probability of adversary's success in producing a forgery than the XOR-MAC modes.

1 Introduction

No one said this was an easy game !
Paul van Oorschot, March 1999.

A long-standing goal in the design of block encryption modes has been the ability to provide message-integrity protection with simple Manipulation Detection Code (MDC) functions, such as the exclusive-or, cyclic redundancy code (CRC), or even constant functions [9, 33, 12, 15]. Most attempts to achieve this goal focused on different variations of the Cipher Block Chaining (CBC) mode of encryption, which is the most common block-encryption mode in use. To date, most attempts failed [14].

*This work was performed in part while this author was on sabbatical leave from the University of Maryland, Department of Electrical and Computer Engineering, College Park, Maryland 20742.

In this paper, we define the eXtended Ciphertext Block Chaining (XCBC) modes that can be used with an exclusive-or function to provide the authentication of encrypted messages in a single pass over the data. These modes detect integrity violations at a low cost in performance, power, and implementation, and can be executed in a parallel or pipelined manner. They provide authentication of encrypted messages in real-time, without the need for an additional processing path over the input data, and can be executed in a parallel or pipelined manner. The performance and security of these modes scales directly with the performance and security of the underlying block encryption function since separate cryptographic primitives, such as hash functions, are unnecessary. We present some preliminary performance measurements of one of these modes via-a-vis CBC-MD5, CBC-HMAC-SHA1, and CBC-UMAC-STD30.

We also present the XECB modes for message authentication (i.e., XECB-MAC modes) and their salient properties. These message authentication modes have all the operational properties of the XOR message authentication (XOR-MAC) modes (e.g., they can operate in a fully parallel and pipelined manner, and support incremental updates and out-of-order verification [3], and have better performance. That is, the XECB modes use only about half the number of block encryption required by the XOR-MAC modes. However, the XECB-MAC modes have higher bounds on the adversary's success of producing a forgery than those of the XOR-MAC modes. The XECB modes are intended for use either stand-alone to protect the integrity of plaintext messages, or with encryption modes that have similar properties (e.g., counter-based XOR encryption).

2 An Integrity Mode for Encryption

Preliminaries and Notation. In defining the encryption modes we adopt the approach of Bellare *et al.* (viz., [2, 3, 1]), who show that an encryption mode can be viewed as the triple (E, D, KG), where E is the encryption function, D is the decryption function, and KG is the probabilistic key-generation algorithm. (Similarly, a message authentication (MAC) mode can be viewed as the triple (S, V, KG), where S is the message signing function, V is the message verification function, and KG is the probabilistic key-generation algorithm.) Our encryption (and authentication) modes are implemented with block ciphers, which are modeled with finite families of pseudorandom functions (PRFs) or pseudorandom permutations (PRPs). In this context, a finite family of functions, F, consists of a set of functions and a set of strings (i.e., the set of keys), each string identifying a member function, f. Each function f maps $\{0,1\}^l$ to $\{0,1\}^L$, where l/L denotes the input/output length, and hence we say that F has input/output length l/L. The finite family F is *pseudorandom* if the input-output behavior of a function $f = F_K$, which is identified by key K drawn uniformly at random from the set of keys, "looks random" to someone who does not know K [2]. This means that someone's advantage in distinguishing F from R, which is the set of all functions that map $\{0,1\}^l$ to $\{0,1\}^L$, using q queries of f in time t, is a negligible value, ϵ. Given encryption scheme (E, D, KG), we denote the use of the key K in the encryption of a plaintext string x by $E^{F_K}(x)$, and in the decryption of ciphertext string y by $D^{F_K}(y)$.

Given and encryption scheme or mode $\Pi = (E, D, KG)$, the most common method used to detect modifications of encrypted messages applies a MDC function g (e.g., a non-keyed hash, cyclic redundancy code (CRC), bitwise exclusive-or function [23]) to a plaintext message and concatenates the result with the plaintext before encryption with E. A message thus encrypted can be decrypted and accepted as valid only after the integrity check is passed; i.e., after decryption with D, the concatenated value of function g is removed from the plaintext, and the check passes only if this value matches that obtained by applying the MDC function to the remaining plaintext [9, 33, 12, 23]. If the integrity check is not passed, a special failure indicator, denoted by $Null$ herein, is returned. This method[1] has been used in commercial systems such as Kerberos V5 [27, 29] and DCE [10, 29], among others. The encryption scheme obtained by using this method is denoted by Π-g = (E-g,D-g,KG). In this mode, we denote the use of the key K in the encryption of a plaintext string x by E^{F_K}-g(x), and in the decryption of ciphertext string y by D^{F_K}-g(y).

A design goal for Π-g = (E-g, D-g, KG) modes is to find the simplest encryption mode Π = (E,D,KG) (e.g., comparable to the CBC modes) such that, when this mode in used with a simple, non-cryptographic MDC function g (e.g., as simple as a bitwise exclusive-or function), message encryption is protected against *existential forgeries.* For any key K, a forgery is any ciphertext message that is not the output of E^{F_K}-g. An existential forgery (EF) is a forgery that passes the integrity check of D^{F_K}-g upon decryption; i.e., for forgery y', D^{F_K}-g(y') $\neq Null$, where $Null$ is a failure indicator. Note that the plaintext outcome of an existential forgery need not be known to the forgerer. It is sufficient that the receiver of a forged ciphertext decrypt the forgery correctly.

Forgeries can be created in many ways, for example (1) by modifying the ciphertexts of legitimate messages whose plaintext may be known by the forgerer, (2) by including arbitrary, never-seen-before, strings into existing ciphertexts, or (3) by combinations of the two. Ciphertexts of legitimate message encryptions can be obtained as a result of different attack scenarios, such as chosen-plaintext attacks (CPA) or ciphertext-only attacks (COA). Hence, message integrity attacks can be defined as a combination of attack goals (e.g., EF) and attack scenarios (e.g., CPA), as suggested by Naor [24].

Message Integrity Attack: the EF-CPA Combination. The attack is defined by a protocol between an adversary A and an oracle O as follows.

1. A and O select encryption mode Π-g = (E-g,D-g,KG), and O selects, uniformly at random, a key K of KG.
2. A sends encryption queries (i.e., plaintext messages to be encrypted) x^p, $p = 1, \cdots, q_e$, to the encryption function of O. O responds to A by returning $y^p = E^{F_K}\text{-}g(x^p)$, $p = 1, \cdots, q_e$, where x^p are A's chosen plaintext messages. A records both its encryption queries and O's responses to them.
3. After receiving O's encryption responses, A forges a collection of ciphertexts $y'^i, 1 \leq i \leq q_v$ where $y'^i \neq y^p, \forall p = 1, \cdots, q_e$, and sends each decryption query y'^i to the decryption function of O. O returns a success or failure indicator to A, depending on whether of $D^{F_K}\text{-}g(y'^i) \neq Null$.

Adversary A is successful if at least one $D^{F_K}\text{-}g(y'^i) \neq Null$ for $1 \leq i \leq q_v$; i.e., y'^i is an existential forgery. The mode Π-g = (E-g,D-g,KG) is said to be secure against a message-integrity attack if the probability of an existential forgery in a chosen-plaintext attack is negligible. (We use the notion of negligible probability in the same sense as that of Naor and Reingold [24].)

Attack Parameters. A is allowed q_e encryption queries (i.e., queries to E^{F_K}-g), and q_v decryption queries (i.e., queries to D^{F_K}-g) totaling $\mu_e + \mu_v$ bits, and taking time $t_e + t_v$.

Parameters q_e, μ_e, t_e are bound by the parameters defining the chosen-plaintext security of Π = (E,D,KG) in a left-or-right sense [1], for instance, and a constant c' defining the speed of the function g. (Briefly, the

[1] Note that other methods for protecting the integrity of encrypted messages exist; i.e., taking the keyed MAC of a message using a secret key before encrypting the message with a separate secret key [23]. These methods require two passes over the message data, require more power, and are more complex to implement than the modes we envision, and thus are less relevant for to our goals.

notion of security in the left-or-right sense allows adversary A to query the encryption function of oracle Q with q' queries of the form (x_l, x_r), where x_l and x_r are equal-length plaintext messages. O flips a coin and decides to encrypt the left or right messages of the q_e queries depending on the outcome of the coin flip. The scheme is considered to be secure if, after receiving the q' encryption queries totaling μ' bits, and taking time t', adversary A cannot obtain a non-negligible advantage (i.e., greater than ϵ') in distinguishing which side of the queries was chosen for encryption by the oracle.) In proving the security of scheme Π in a left-or-right sense, parameters $(q', \mu', t', \epsilon')$ are expressed in terms of the given parameters (q, t, ϵ) of the family of pseudorandom functions (or permutations) F.

Parameters q_v, μ_v, t_v are bound by the desired probability of adversary's success and by those of F. $q_v > 0$ since A must be allowed verification queries. Otherwise, A cannot test whether his forgeries are correct, since A does not know key K.

The message-integrity attack defined above is not weaker than an adaptive one in the sense that the success probability of adversary A bounds from above the success probability of another adversary A' that intersperses the q_e encryption and q_v verification queries; i.e., the adversary is allowed to make his choice of forgery after seeing the result of legitimate encryptions and other forgeries. (This has been shown for chosen-message attacks against MAC functions [3], but the same argument holds here.) To date, this is the strongest of the known goal-attack combinations against the integrity (authentication) of encrypted messages [4, 16, 17].

3 Definition of the XCBC and XCBC-XOR Modes

In the encryption modes presented below, the key generation algorithm, KG, outputs a random, uniformly distributed, k-bit string or key K for the underlying PRP family F, thereby specifying $f = F_K$ and $f^{-1} = F_K^{-1}$ of l-bits to l-bits. If a separate second key is needed in a mode, then a new string or key K' is generated by KG identifying $f' = F_{K'}$ and $f'^{-1} = F_{K'}^{-1}$. The plaintext message to be encrypted is partitioned into a sequence of l-bit blocks (padding is done first, if necessary), $x = x_1 \cdots x_n$. Throughout this paper, $\oplus$ is the *exclusive-or* operator and $+$ represents *modulo* 2^l *addition*.

Stateless XCBC Mode (XCBC\$)
The encryption and decryption functions of the stateless mode,
$\mathcal{E}{-}XCBC\$^{F_K}(x)$ and $\mathcal{D}{-}XCBC\$^{F_K}(y)$, are defined as follows.

function $\mathcal{E}{-}\text{XCBC}\$^f(x)$	**function** $\mathcal{D}{-}\text{XCBC}\$^f(y)$
$r_0 \leftarrow \{0,1\}^l$	Parse y as $y_0 \| y_1 \cdots y_n$
$y_0 = f(r_0);\ z_0 = f'(r_0)$	$r_0 = f^{-1}(y_0);\ z_0 = f'(r_0)$
for $i = 1, \cdots, n$ **do** $\{$	**for** $i = 1, \cdots, n$ **do** $\{$
$z_i = f(x_i \oplus z_{i-1})$	$z_i = y_i - i \times r_0$
$y_i = z_i + i \times r_0$ $\}$	$x_i = f^{-1}(z_i) \oplus z_{i-1}$ $\}$
return $y = y_0 \| y_1 y_2 \cdots y_n$	**return** $x = x_1 x_2 \cdots x_n$

Stateful XCBC Mode (XCBC)
The encryption and decryption functions of the stateful mode,
$\mathcal{E}{-}XCBC^{F_K}(x, ctr)$ and $\mathcal{D}{-}XCBC^{F_K}(y)$, are defined as follows.

function $\mathcal{E}$–XCBC$^f(x, ctr)$ $r_0 = f(ctr);\ z_0 = f'(r_0)$ **for** $i = 1, \cdots, n$ **do** { $z_i = f(x_i \oplus z_{i-1})$ $y_i = z_i + i \times r_0$ } $ctr' \leftarrow ctr + 1$ $y = ctr\|\|y_1 y_2 \cdots y_n$ **return** y	**function** $\mathcal{D}$–XCBC$^f(y)$ Parse y as $ctr\|\|y_1 \cdots y_n$ $r_0 = f(ctr);\ z_0 = f'(r_0)$ **for** $i = 1, \cdots, n$ **do** { $z_i = y_i - i \times r_0$ $x_i = f^{-1}(z_i) \oplus z_{i-1}$ } **return** $x = x_1 x_2 \cdots x_n$

Note that in the XCBC mode the counter ctr can be initialized to a known constant such as -1 by the sender. ctr' represents the updated ctr value.

The encryption modes defined above use the same *block chaining sequence* as that used for the traditional CBC mode, namely $z_i = f(x_i \oplus z_{i-1})$, where z_0 is the initialization vector, x_i is the plaintext and z_i is the ciphertext of block $i, i = 1, \cdots, n$. In contrast with the traditional CBC mode, the value of z_i is not revealed outside the encryption modes, and, for this reason, z_i is called a *hidden* ciphertext block. The actual ciphertext output, y_i, of the XCBC mode is defined using extra randomization, namely $y_i = z_i + i \times r_0$, where $i \times r_0$ is the *modulo* 2^l *addition* of the random, uniformly distributed, variable r_0, i times to itself; i.e., $i \times r_0 \stackrel{def}{=} \underbrace{r_0 + \cdots + r_0}_{i\ times}$. (In systems where the modular multiplication with a constant is fast, $i \times r_0$ can be implemented as a per-block multiplication.) It should be noted that other functions, or combinations of functions, not just the incremental addition modulo 2^l of r_0, could be used to define the ciphertext block sequence y_i; e.g., subtraction modulo 2^l (viz., also *Support for Multiple Encryption Modes* in the next section). Note that these functions may allow the low-order bits of some z_i's to become known.

In *stateless* implementations of the XCBC modes, $r_0 \leftarrow \{0,1\}^l$; i.e., r_0 is initialized to a random, uniformly distributed, l-bit value for every message. The value of r_0 is sent by the sender to the receiver as $y_0 = f(r_0)$. In contrast, in *stateful* implementations, a counter, ctr, is initialized to a new l-bit constant (e.g., -1) for every key, K, and incremented on every message encryption. In both stateless and stateful implementations, the initialization vector z_0 is set to $f'(r_0)$, which is independent of r_0 and, just as r_0, remains secret. Alternate stateful implementations are possible whereby the counter ctr and the secret r_0 are shared by both the sender and receiver. As a consequence, the sender need not compute y_0 and send its value to the receiver. We also note that other functions, not just $f' = F_{K'}$, can be used for generating the secret initialization vector z_0. For instance, $z_0 = f(r_0 + 1)$, in which case only a single key, K, is used. It is important that the encryption of these functions of r_0 produce a pseudorandom value for z_0 that is independent of r_0, and remains secret.

XCBC-XOR Modes. To illustrate the properties of the XCBC modes in integrity attacks, we choose $g(x) = z_0 \oplus x_1 \oplus \cdots \oplus x_n$ for plaintext $x = x_1 \cdots x_n$, where z_0 is internally defined by both the XCBC\$ and XCBC modes. In this example, block $g(x)$ is appended to the *end* of a n-block message plaintext x, and hence block $x_{n+1} = z_0 \oplus x_1 \oplus \cdots \oplus x_n$. For this choice of $g(x)$, the integrity check performed at decryption becomes $z_0 \oplus x_1 \oplus \cdots \oplus x_n = f^{-1}(z_{n+1}) \oplus z_n$, where $z_{n+1} = y_{n+1} - (n+1) \times r_0$, and $z_n = y_n - n \times r_0$. An adversary is successful if the forged ciphertext produced in the attack defined above passes this check for at least one of the q_v verification queries. Hence, an upper bound for the probability of adversary's success represents a quantitative measure of the integrity properties of the XCBC modes with respect to the choice of function $g(x) = z_0 \oplus x_1 \oplus \cdots \oplus x_n$.

Throughout this paper, the stateless and stateful encryption modes Π-g obtained by the use of schemes Π = XCBC\$ or Π = XCBC with function $g(x) = z_0 \oplus x_1 \oplus \cdots \oplus x_n$ are denoted by XCBC\$-XOR and XCBC-XOR, respectively.

Examples of Other Encryption Modes that Preserve Message Integrity. Few modes of encryption Π-g, where g is a simple, non-cryptographic MDC function, are known that are EF-CPA secure. The performance characteristics of most of these modes do not satisfy all our goals, however. For example, when implemented with the CBC mode and used to encrypt messages consisting of an integer number of l-bit blocks (possibly after padding), the Variable Input Length (VIL) cipher of Bellare and Rogaway [5, 6] can be shown to be EF-CPA secure when using simple non-cryptographic MDC functions g,[2] such as those for the bitwise exclusive-or, CRCs, addition *modulo* $2^l - 1$, the selection of a single constant-filled block or just block x_1 of every message, whose output is appended *to the end* of the message before encryption. However, the VIL cipher uses two sequential passes over its input and, thus, its performance is lower than those of single-pass schemes using hash functions or separate-key MACs.

Katz and Yung [16] proposed an interesting single-pass encryption mode, called the Related Plaintext Chaining (RPC), that is EF-CPA secure when using a non-cryptographic MDC function g consisting only of message start and end tokens. RPC has several important operational advantages, such as full parallelization, incremental updates, out-of-order processing, and low upper bound on the probability of adversary's success in producing a forgery.[3] However, it wastes a substantial amount of throughput since it encrypts the block sequence number and message data in the same block. This may make the selection of modern hash functions as the MDC function g for common encryption modes, such as CBC, a superior performance alternative, at least for sequential implementations. Similarly the use of modern MACs, such as the UMAC, with a separate key may also produce better overall throughput performance than RPC when used with common encryption modes.

More recently, C.S. Jutla [20] proposed an interesting scheme in which the output blocks z_i of CBC encryption are modified by (i.e., bitwise exclusive-or operations) with a sequence S_i of pairwise independent elements. The complexity of this mode is superior to that of both VIL and RPC; i.e., this mode exceeds the complexity of single-pass schemes only by $\Omega(\log n)$ block encryptions, where n is the number of plaintext blocks of a message. This is shown to be a lower bound for a model where the only operations allowed in addition to block encryptions are linear operations over $(GF2)^l$ (i.e., bitwise exclusive-or operations on l-bit blocks). Jutla also proposes a slightly different model that, just as the XCBC modes, also allows modular additions. In this model, $S_i = (i \times r_0 + r_1) mod\ p$, where r_0, r_1 are random values and p is prime, and the complexity $n+3$. In contrast with Jutla's scheme, the elements of the XCBC sequence, $S_i = (i \times r_0) mod\ 2^l$, are not pairwise independent, and the complexity is $n+2$. Also, the performance of the required modular 2^l additions is somewhat better than that of *mod p* additions, where p is prime. However, the pairwise independence of Julta's S_i sequence should yield a somewhat tighter bound on the probability of successful forgery, illustrating, yet again, a fundamental tradeoff between performance and security.

4 Properties of the XCBC Modes

The XCBC modes have notable secrecy and integrity properties in several areas.

[2] This is neither the reason VIL was introduced nor its intended use.

[3] RPC preserves the block ordering in the same way as the XOR-MAC [3]; i.e., it reserves part of every plaintext block for the block sequence number. It also shares the same operational advantages and disadvantages as the XOR-MAC.

1. Support for Message Integrity. The XCBC modes require only a single cryptographic primitive, namely the block cipher that is necessary for encryption, to maintain integrity. Further, other functions (i.e., not just the $g(x)$ function defined above), such as the CRCs and modular addition checksums, can also be used with the XCBC modes for protection against message integrity attacks (unlike the original CBC and PCBC modes).

2. Support for Real-Time Message Authentication.

Both the stateless and stateful XCBC modes can be used with $g(x) = z_0 \oplus x_1 \oplus \cdots \oplus x_n$ for real-time message sources in which (1) the message length remains unknown until the message ends, (2) the beginning of message authentication cannot be deferred until the end of message receipt, and (3) only small, fix-sized, buffers for authentication processing are available, as would be the case with most low-cost, low-power, hardware implementations. Also the XCBC modes can produce good Message Authentication Codes (MACs). For example, a Double MAC approach [25] can be used for both the XCBC$ (XCBC) modes to obtain good MACs.

3. Support for Multiple Encryption Modes. The definition of the ciphertext generation y_i from the hidden ciphertext block z_i, (i.e., the output of the internal CBC encryption mode), can be changed to obtain other modes of encryption that may be faster or have better security bounds. For example,

- $y_i = z_i \oplus (i \times r_0)$ in which one of the additions *mod* 2^l per block is replaced by an exclusive-or;
- $y_i = z_i + r_i$, where $r_i = a^i \times r_0$ is a linear congruence sequence with multiplier a. The multiplier a can be chosen so that the sequence passes spectral tests to whatever degree of accuracy is deemed necessary. Examples of good multipliers are readily available in the literature [18]. This mode may have a better upper bound for the probability of breaking the integrity condition.

We also note that the traditional PCBC modes can also be used to generate an XPCBC mode in the same way as the XCBC mode was generated based on the traditional CBC mode above. The conventional initialization-vector attacks defined by Voydock and Kent [32] are also countered by the use of z_0 as the initialization vector.

The XCBC modes capture the history of the message encryption only from the previous block, just as the CBC modes. However, in contrast to the original CBC modes, the XCBC modes add an extra randomization step which is the key ingredient that assures that the integrity check can pass only with low probability.

4. Support for Parallel or Pipelined Encryption. The choice of $g(x) = z_0 \oplus x_1 \oplus \cdots \oplus x_n$, allows the parallel or pipelined implementation of the XCBC modes. Other non-cryptographic MDC functions $g(x)$ would also allow such implementation, since they be executed in a parallel or a pipelined manner (by definition). For example, for parallel execution using $g(x)$, each plaintext message x is partitioned into L segments, $x^{(1)} \cdots x^{(L)}$ each of length n_s, $s = 1, \cdots, L$, after customary block-level padding (n.b., this L should not be confused with the output length of a PRF, which is typically denoted by L, also). Each segment, $x^{(s)}, s = 1, \cdots, L$, consists of one or more l-bit blocks, and if $g(x^{(s)}) = z_0^{(s)} \oplus x_1^{(s)} \oplus \cdots \oplus x_{n_s}^{(s)}$ is used, then an additional l-bit block is included in each segment. Each segment is encrypted/decrypted in parallel on a separate processor.

In parallel or pipelined implementations of the XCBC modes, the initialization and computation of the block chaining sequence is performed on a per-segment basis starting with a common value of r_0, which is a random, uniformly distributed, l-bit value for every message. Also, the per-message value y_0 is computed as $y_0 \leftarrow f(r_0)$ in stateless implementations. The initialization of the block chaining sequence for message segment s can be $r_0^{(s)} = r_0 + s$, $z_0^{(s)} = f'(r_0^{(s)})$, and the encryption sequence can be $z_i^{(s)} = f(x_i^{(s)} \oplus z_{i-1}^{(s)}), y_i^{(s)} = z_i^{(s)} + i \times r_0^{(s)}$. In stateful implementations ctr is updated to $ctr + L$ after the encryption of each message. (Other functions, not just addition modulo 2^l, can be used for the computation of the per-segment, block chaining sequence, and initialization sequence can be used for $r_0^{(s)}$ and $z_0^{(s)}$.)

The encrypted segments of a message are assembled to form the message ciphertext. Segment assembly encodes the number of segments L, the length of each segment n_s and, implicitly, the segment sequence in the message (e.g., all can be found in the ASN.1 encoding). If the segments of a message have different lengths, segment assembly is also synchronized with the end of each segment encryption or decryption within a message.

At decryption, the parsing of the message ciphertext yields the message length, L, segment sequence number, s, and the length of each segment, n_s. Message integrity is maintained both on a per segment and per message basis by performing the per-segment integrity check; if $g(x) = z_0 \oplus x_1 \oplus \cdots \oplus x_n$, the per-segment check is $z_0^{(s)} \oplus x_1^{(s)} \oplus \cdots \oplus x_{n_s}^{(s)} = f^{-1}(z_{n_s+1}^{(s)}) \oplus z_{n_s}^{(s)}$ where $z_{n_s+1}^{(s)} = y_{n_s+1}^{(s)} - (n_s + 1) \times r_0^{(s)}$ and $z_{n_s}^{(s)} = y_{n_s}^{(s)} - n_s \times r_0^{(s)}$. Failure of any per-segment integrity check, which also detects out-of-sequence segments and message-length modifications, signals a message integrity violation.

We illustrate a parallel implementation of the XCBC modes below.

Stateless Parallel XCBC Mode (pXCBC\$)
The encryption and decryption functions of the stateless mode, $\mathcal{E}-pXCBC\$^{F_K}(x)$ and $\mathcal{D}-pXCBC\$^{F_K}(y)$, are defined as follows.

function $\mathcal{E}$−pXCBC\$$^f(x)$
partition x into L segments $x^{(s)}$
each of length n_s;
$r_0 \leftarrow \{0,1\}^l$; $y_0 = f(r_0)$;
for segment $s, s = 1, \cdots, L$, **do** {
$r_0^{(s)} = r_0 + s,\ z_0^{(s)} = f'(r_0^{(s)})$
for $i = 1, \cdots, n_s$ **do** {
$z_i^{(s)} = f(x_i^{(s)} \oplus z_{i-1}^{(s)})$
$y_i^{(s)} = z_i^{(s)} + i \times r_0^{(s)}$ }
$y^{(s)} = y_1^{(s)} \cdots y_{n_s}^{(s)}$ }
assemble $y = y_0 || y^{(1)} \cdots y^{(L)}$;
return y.

function $\mathcal{D}$−pXCBC\$$^f(y)$
parse y into y_0 and L segments $y^{(s)}$
each of length n_s;
$r_0 = f^{-1}(y_0)$
for segment $s, s = 1, \cdots, L$ **do** {
Parse $y^{(s)}$ as $y_1^{(s)} \cdots y_{n_s}^{(s)}$
$r_0^{(s)} = r_0 + s;\ z_0^{(s)} = f'(r_0^{(s)})$
for $i = 1, \cdots, n_s$ **do** {
$z_i^{(s)} = y_i^{(s)} - i \times r_0^{(s)}$
$x_i^{(s)} = f^{-1}(z_i^{(s)}) \oplus z_{i-1}^{(s)}$ }
$x^{(s)} = x_1^{(s)} \cdots x_{n_s}^{(s)}$ }
assemble $x = x^{(1)} \cdots x^{(L)}$;
return x.

Stateful Parallel XCBC Mode (pXCBC)
The encryption and decryption functions of the stateful mode, $\mathcal{E}-pXCBC^{F_K}(x, ctr)$ and $\mathcal{D}-pXCBC^{F_K}(y)$, are defined as follows.

function $\mathcal{E}$−pXCBC$^f(x, ctr)$
partition x into L segments $x^{(s)}$
each of length n_s;
$r_0 = f(ctr)$;
for segment $s, s = 1, \cdots, L$, **do** {
$r_0^{(s)} = r_0 + s$; $z_0^{(s)} = f'(r_0^{(s)})$
for $i = 1, \cdots, n_s$ **do** {
$z_i^{(s)} = f(x_i^{(s)} \oplus z_{i-1}^{(s)})$
$y_i^{(s)} = z_i^{(s)} + i \times r_0^{(s)}$ }
$y^{(s)} = y_1^{(s)} \cdots y_{n_s}^{(s)}$ }
assemble $y = ctr || y^{(1)} \cdots y^{(L)}$;
$ctr' \leftarrow ctr + L$;
return y.

function $\mathcal{D}$−pXCBC$^f(y)$
parse y into ctr and L segments $y^{(s)}$
each of length n_s;
$r_0 = f(ctr)$
for segment $s, s = 1, \cdots, L$ **do** {
Parse $y^{(s)}$ as $y_1^{(s)} \cdots y_{n_s}^{(s)}$
$r_0^{(s)} = r_0 + s$; $z_0^{(s)} = f'(r_0^{(s)})$
for $i = 1, \cdots, n_s$ **do** {
$z_i^{(s)} = y_i^{(s)} - i \times r_0^{(s)}$
$x_i^{(s)} = f^{-1}(z_i^{(s)}) \oplus z_{i-1}^{(s)}$ }
$x^{(s)} = x_1^{(s)} \cdots x_{n_s}^{(s)}$ }
assemble $x = x^{(1)} \cdots x^{(L)}$;
return x.

Note that in the XCBC mode the counter ctr can be initialized to a known constant such as -1 by the sender. ctr' represents the updated ctr value.

5. Incremental Updates of Encrypted Data. The segmentation of a message used for parallel and pipelined implementation of the XCBC modes can also be used in sequential encryption of data structures (e.g., a file, a message) whenever incremental updates of data structures are anticipated. Such segmentation enables the localization of the decryption, plaintext update, and encryption to single segments saving the decryption and encryption of other segments unaffected by the updates. Note that message integrity is retained after such incremental updates.

6. Resistance to Key Attacks. Resistance to exhaustive key-guessing attacks can be implemented in a similar manner as that of DESX [28].

5 Definition of the XECB Authentication Modes

In this section, we introduce new Message Authentication Modes (MACs) that counter adaptive chosen-message attacks [3]. We call these MACs the eXtended Electronic Code Book MACs, or XECB-MACs. The XECB-MAC modes have all the properties of the XOR MACs [3] plus they do not waste half of the block size for recording the block position. First we define these MACs, and then we present their properties. Several variants of such MACs can be derived, and here we present a stateless version of XECB-MAC, namely the XECB$-MAC, and a stateful version, namely the XECB-MAC.

A stateless implementation of the XECB$-MAC uses as initialization sequence $r_0 \leftarrow \{0,1\}^l$ and $y_0 = f(r_0)$. Then, each block of message x, namely $x_i, 1 \leq i \leq n, n = |x|$ is randomized as $x_i + i \times r_0$, and the result is input to function f; i.e., $y_i = f(x_i + i \times r_0)$. These values, $y_1, \cdots, y_n$, and r_0 are exclusive-OR-ed to generate the authentication tag:

$$w = r_0 \oplus y_1 \oplus \cdots \oplus y_n.$$

The algorithm outputs the pair (y_0, w). For verification, the attacker submits a forgery $x = x_1 \cdots x_n$

and a forged pair (y_0, w).[4] The algorithm proceeds with computing $r_0 = f^{-1}(y_0)$, then computes $y_i = f(x_i + i \times r_0), \forall i, 1 \leq i \leq n$ and the authentication tag $w' = r_0 \oplus y_1 \oplus \cdots \oplus y_n$. The algorithm outputs a bit that is either 1, if the forged authentication tag is correct, namely $w = w'$, or 0, otherwise.

In the stateful mode, the signer maintains state across consecutive signing requests in the form of a counter (ctr). Hence, the initialization phase is defined as $r_0 = f(ctr)$. Then, for each message block, $y_i = f(x_i + i \times r_0), \forall i, 1 \leq i \leq n, n = |x|$. The authentication tag is then defined as

$$w = r_0 \oplus y_1 \oplus \cdots \oplus y_n.$$

The algorithm outputs the pair (ctr, w). For verification, the attacker submits a forgery $x = x_1 \cdots x_n$ and a forged pair (ctr, w). The algorithm proceeds with computing $r_0 = f(ctr)$, then computes $y_i = f(x_i + i \times r_0), \forall i, 1 \leq i \leq n$ and the tag $w' = r_0 \oplus y_1 \oplus \cdots \oplus y_n$. The algorithm outputs a bit that is either 1, if the forged authentication tag is correct, namely $w = w'$, or 0, otherwise.

The concrete implementation for the signing and verifying algorithms for the stateless and stateful XECB-MAC modes is defined as follows.

Stateless XECB-MAC Mode (XECB\$-MAC)

function Sign-XECB\$-MAC$^f(x)$	**function** Verify-XECB\$-MAC$^f(x, y_0, w)$
$r_0 \leftarrow \{0,1\}^l$	$r_0 = f^{-1}(y_0)$
$y_0 = f(r_0)$	**for** $i = 1, \cdots, n$ **do** $\{$
for $i = 1, \cdots, n$ **do** $\{$	$y_i = f(x_i + i \times r_0)$ $\}$
$y_i = f(x_i + i \times r_0)$ $\}$	$w' = r_0 \oplus y_1 \oplus \cdots \oplus y_n$
$w = r_0 \oplus y_1 \oplus \cdots \oplus y_n$	**if** $w = w'$ **then return** 1
return (y_0, w)	**else return** 0.

Stateful XECB-MAC Mode (XECB-MAC)

function Sign-XECB-MAC$^f(ctr, x)$	**function** Verify-XECB-MAC$^f(x, ctr, w)$
$r_0 = f(ctr)$	$r_0 = f(ctr)$
for $i = 1, \cdots, n$ **do** $\{$	**for** $i = 1, \cdots, n$ **do** $\{$
$y_i = f(x_i + i \times r_0)$ $\}$	$y_i = f(x_i + i \times y_0)$ $\}$
$w = r_0 \oplus y_1 \oplus \cdots \oplus y_n$	$w' = r_0 \oplus y_1 \oplus \cdots \oplus y_n$
$ctr' \leftarrow ctr + 1$	**if** $w = w'$ **then return** 1
return (ctr, w)	**else return** 0.

Note that in the XECB mode the counter ctr can be initialized to a known constant such as -1 by the sender. ctr' represents the updated ctr value.

The stateless XECB-MAC\$ mode requires the use of PRPs while the stateful XECB-MAC modes can be implemented using PRFs.

It should be noted that the implementation of the XECB-MAC modes can be performed in software, hardware, or software with hardware support. Implementations can be in general-purpose computers or

[4]The forgery (x, y_0, w) is not a previously signed query. Note also that the length n of the forged message needs not be equal to the length of any signed message.

in dedicated hardware devices and software. We now present the properties of the stateless and stateful XECB-MAC modes.

6 Properties of the XECB Authentication Modes

1. Security. The XECB authentication modes are intended to be secure against adaptive chosen-message (q_s, q_v)-attacks [3]. These attacks are similar to the message integrity attack defined in this paper. The only difference is that instead of q_e (encryption) queries totaling μ_e bits and taking time t_e, this attack uses q_s (signature) queries, totaling μ_s bits and taking time t_s. Theorem 3 below shows the security bounds for these modes against adaptive chosen-message attacks. The XECB modes have higher upper bounds on the adversary's success in producing a forgery than those of the XOR-MAC modes.

2. Parallel and Pipelined Operation. Function f (e.g., DES, RC6) computations on different blocks can be made in a *fully parallel* or *pipelined* manner; i.e., it can exploit any degree of parallelism or pipelining available at the sender or receiver. This property is important for high speed networks and in both hardware and software implementations.

3. Incremental Updates. The XECB-MAC modes are incremental with respect to block replacement, e.g., a block x_i of a long message is replaced with a new value x'_i. For instance, let us consider the stateless mode. Let the two messages have the same random block r_0; hence, the authentication tag of the new message, w', is obtained from the authentication tag of the previous message, w, by the following formula: $w' = w \oplus f(x_i + i \times r_0) \oplus f(x'_i + i \times r_0)$. The replacement property can be easily extended to insertion and deletion of blocks.

4. Out-of-order Verification. The verification of the authentication tag can proceed even if the blocks of the message arrive out of order as long as each block is accompanied by its index and the first block has been retrieved.

5. Block Encryption Computations. In contrast to the XOR-MAC modes, where the number of block encryption computations is twice the number of block encryption computations for CBC-MAC [3], the number of block encryption computations in the XECB-MAC modes is the same as the number of block encryption computations for the CBC-MAC. While in sequential implementations the performance of XECB-MACs is expected to be just slightly lower than the performance of the CBC-MAC (because of the two modular additions per block vs. one exclusive-OR for CBC-MAC), the XECB mode can take advantage of parallelism or pipelining in an architecture-independent manner; i.e., the number of processors available need not be known apriori – a significant feature available only in few modes such as the XOR-MAC. This property, the out-of-order and incremental computation are especially important in hardware implementations, particularly in high-speed networks and for the internet. For this reason, the use of the XECB-MAC modes appears to be more appropriate than that of the XOR-MAC for the integrity protection of messages encrypted under fully parallel or pipelined encryption schemes such as the XORrC [13], which is a random-counter variant of the counter-based XOR encryption mode [1].

7 Security Considerations

In this section, we provide evidence for the security of the XCBC modes against both adaptive chosen-plaintext and message-integrity attacks. We also present the security of the XECB modes in adaptive chosen-message attacks.

We first address the security (i.e., secrecy) of the XCBC\$ mode against adaptive chosen-plaintext attacks. The theorems and proofs that demonstrate that the stateful mode (XCBC) and the two-key variations are secure in a left-or-right sense [1] are similar to that for the XCBC\$ mode and, therefore, will be omitted.

The Lemma and Theorem below, which establish the security (i.e., secrecy) of the XCBC\$ mode are restatements of Lemma 16 and Theorem 17 respectively, which are presented for the CBC mode in the full version of the Bellare *et al.* paper ([1]). The proof of the Lemma and Theorem are similar to those for the CBC mode and hence are omitted.

Lemma 1 [Upper bound on the security of the XCBC\$ mode in random function model]
Let $XCBC\$^R$ be the implementation of the XCBC\$ mode with the family of random functions $R(l,l)$. Let A be any adversary attacking $XCBC\$^R$ in the left-or-right sense, making at most q' queries, totaling at most μ' bits. Then, the adversary's advantage is

$$Adv_A^{lr} \leq \delta_{XCBC\$} \stackrel{def}{=} \left(\frac{\mu'^2}{l^2} - \frac{\mu'}{l}\right)\frac{1}{2^l}.$$

The following theorem defines the security of the XCBC\$ mode against an adaptive chosen-plaintext attack when the XCBC\$ mode is implemented with a (q,t,ϵ)-pseudorandom function family F. F is (q,t,ϵ)-pseudorandom, or (q,t,ϵ)-secure, if an adversary (1) spends time t to evaluate $f = F_K$ at q input points via adaptively chosen queries, and (2) has a negligible advantage bounded by ϵ over simple guessing in distinguishing the output of f from that of a function chosen at random from R.

Theorem 1 [Security of XCBC\$ against Adaptive Chosen-Plaintext Attacks]
Suppose F is a (t,q,ϵ)-secure PRF family with block length l. There is a constant $c > 0$ such that for any number of queries q_e totaling μ' bits of memory and taking time t', the $XCBC\$(F)$ is (t',q',μ',ϵ')-secure in the left-or-right sense, for $\mu' = q'l$, $t' = t - c\mu'$, and $\epsilon' = 2\epsilon + \delta_{XCBC\$}$ where $\delta_{XCBC\$} \stackrel{def}{=} \left(\frac{\mu'^2}{l^2} - \frac{\mu'}{l}\right)\frac{1}{2^l}$.

The XCBC\$ and XCBC modes should really be analyzed assuming F is a PRP family (not a PRF family), and hence one needs to apply the results of Proposition 8 of Bellare *et al.* [1] to the results of Theorem 1 (and also of Theorems 2-3 below). A similar lemma and theorem hold for chosen-plaintext attacks in a real-or-random sense, as defined by Bellare *et al.* [1].

In establishing the security of the XCBC\$ mode against the message-integrity attack, let the parameters used in the attack be bound as follows: $q_e \leq q'$, since the XCBC\$ scheme is also chosen-plaintext secure, $t_e + t_v \leq t$, and $\mu'' = \mu_e + \mu_v \leq ql$. Let the forgery verification parameters q_v, μ_v, t_v be chosen within the constraints of these bounds and to obtain the desired $Pr_{f \stackrel{R}{\leftarrow} F}[Succ]$. □

Theorem 2 [Security of XCBC\$-XOR against a Message-Integrity Attack]
Suppose F is a (t,q,ϵ)-secure PRF family with block length l. The mode XCBC\$-XOR is secure against a message-integrity attack consisting of $q_e + q_v$ queries, totaling $\mu_e + \mu_v \leq ql$ bits, and taking at most $t_e + t_v \leq t$ time; i.e., the probability of adversary's success is

$$Pr_{f \stackrel{R}{\leftarrow} F}[\text{Succ}] \quad \leq \quad \epsilon + \frac{q_e^2}{2^l} + \frac{(q_e+2)\mu_v}{l2^l} + \frac{q_v}{2^l}\left(\frac{\mu_e}{l}\log_2\frac{\mu_e}{l} + \frac{3\mu_e}{l}\right);$$

and, if $m = \max(n_p + 1)$, where n_p, $1 \leq p \leq q_e$, is the number of blocks encrypted in the message p-th message,

$$Pr_{f \stackrel{R}{\leftarrow} F}[\text{Succ}] \quad \leq \quad \epsilon + \frac{q_e^2}{2^l} + \frac{(q_e+2)\mu_v}{l2^l} + \frac{q_v}{2^l}\left(\frac{\mu_e}{l}\log_2 m + \frac{3\mu_e}{l}\right).$$

(The proof of Theorem 2 can be found in Appendix A.) Note that parameters q_e, μ_e, t_e can be easily stated in terms of parameters $(t', q', \mu', \epsilon')$ of Theorem 1 above by introducing a constant c' defining the speed of the XOR function.

Theorem 2 above allows us to estimate the complexity of a message-integrity attack. In a successful attack, $Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[\text{Succ}] \in (\text{negligible}, 1]$. To estimate complexity, we set the probability of success when $f \stackrel{\mathcal{R}}{\leftarrow} R$ to the customary 1/2, and assume that the attack parameters used in the above bound, namely $\frac{\mu_e}{l}, \frac{\mu_v}{l}$, are of the same order or magnitude, namely $2^{\alpha l}$, where $0 < \alpha < 1$. Also, since the shortest message has at least three blocks, $q_e, q_v \leq \lfloor \frac{2^{\alpha l}}{3} \rfloor$.

In this case, by setting

$$\frac{q_e^2}{2^l} + \frac{(q_e + 2)\mu_v}{l 2^l} + \frac{q_v}{2^l}\left(\frac{\mu_e}{l}\log_2\frac{\mu_e}{l} + \frac{3\mu_e}{l}\right) = 1/2,$$

we obtain the equation $2^{2\alpha l}\lfloor\frac{3\alpha l + 13}{9}\rfloor + 2^{\alpha l + 1} = 2^{l-1}$, which allows us to estimate α for different values of l. For example, for $l = 64, \alpha \approx \frac{29}{64}$, for $l = 128, \alpha \approx \frac{61}{128}$, and for $l = 256, \alpha \approx \frac{124}{256}$. Hence, this attack is very close to a square-root attack (i.e., $\alpha \rightarrow \frac{1}{2}$ as l increases). If the maximum length m of the encrypted messages is known, the attack is even closer to a square-root attack.

A variant of Theorem 2 can be proved for the stateful mode. In this case, it can be shown that the probability of successful forgery when q_v verification queries are allowed, totaling at most μ_v bits and using at most time t_v after q_e encryption queries totaling μ_e bits and taking time t_e, is

$$Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[\text{Succ}] \quad \leq \quad \epsilon + \frac{(q_e + 2)\mu_v}{l 2^l} + \frac{q_v}{2^l}\left(\frac{\mu_e}{l}\log_2\frac{\mu_e}{l} + \frac{3\mu_e}{l}\right).$$

Furthermore, similar theorems hold for other stateless modes where $z_0 = f(r_0 + 1)$. The statement and proof for such theorems are similar to the statement and proof for the integrity theorem for the stateless mode, and hence, are omitted.

The XECB\$-MAC mode is intended to be secure against an adaptive chosen-message attack [3] consisting of up to q_s signature queries totaling at most μ_s bits and using time up to t_s, and q_v verification queries totaling at most μ_v bits and using time at most t_v. The security of the XECB\$-MAC mode is established by the following theorem.

Theorem 3 [Security of XEBC\$-MAC in an Adaptive Chosen-Message Attack]
Suppose F is a (t, q, ϵ)-secure PRF family with block length l. The message authentication mode (Sign-XECB$\$^f$, Verify-XECB$\$^f$, KG) is secure against adaptive chosen-message (q_s, q_v) attacks consisting of $q_s + q_v$ queries totaling $\mu_s + \mu_v$ bits and taking at most $t_s + t_v \leq t$ time; i.e., the probability of adversary's success is

$$Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[\text{Succ}] \leq \epsilon + \frac{q_s^2}{2^l} + \frac{(q_s + 2)\mu_v}{l 2^l} + \frac{q_v}{2^l}\left(\frac{\mu_s}{l}\log_2\frac{\mu_s}{l} + \frac{3\mu_s}{l}\right).$$

The proof of this theorem is similar to that of Theorem 2 and hence is omitted. A similar theorem can be provided for the stateful message authentication mode. In this case, it can be shown that the probability of a success is bounded as follows:

$$Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[\text{Succ}] \leq \epsilon + \frac{(q_s + 2)\mu_v}{l 2^l} + \frac{q_v}{2^l}\left(\frac{\mu_s}{l}\log_2\frac{\mu_s}{l} + \frac{3\mu_s}{l}\right).$$

8 Performance Considerations for the XCBC Modes

The performance of the XCBC modes in software implementations is (1) minimally degraded in comparison to that of the original CBC mode [11, 1], and (2) superior to that of the original CBC modes, and most other similar modes, when message integrity is desired.

The XCBC$ modes add the overhead of two block encryption per message (i.e., for generating z_0 and y_0), and two *mod* 2^l additions per message block to the traditional CBC mode with random initialization vectors (or, equivalently, with initialization vectors set to zero and a random number in the first plaintext block [27])[5]. However, the execution of both modulo 2^l additions for the current ciphertext block can always be overlapped with the block encryption of the next block and, hence, at peak speeds there is little perceptible overhead over that of the traditional CBC mode. This compares favorably with the overhead added at peak speeds by an original CBC mode that uses any of the hash functions known to date to provide message integrity. In any case, the dominant performance factor is the throughput achieved by block encryption. An important advantage of the new modes is that their performance scales up nearly identically with that of block encryption; furthermore, hardware implementations of the new modes can make the added overhead imperceptible.

To illustrate the performance characteristics of the XCBC$ scheme in software, we used the *SSLeay* library [30], and conducted some preliminary measurements on a Sun SPARC Ultra 10 IIi processor running the SunOS 5.6 operating system. The processor has a 333 MHz clock, 2 MB of external (off-chip) cache, and 16/16 KB of internal (on-chip) instruction/data cache. We used the version 4.2 of the native C compiler with the -xO2 optimization option. We used a lightly loaded machine for our measurements, and the throughput for each of the eight message sizes was generated by averaging the results of fifty runs.

Our implementation of the addition *mod* 2^l operations was also influenced by the SSLeay implementation of the CBC scheme on 32-bit processors. However, we were able to use 64-bit additions for the XCBC$ scheme. The addition uses the *unsigned long long* type (64 bits) for $i \times r_0 \stackrel{def}{=} \underbrace{r_0 + \cdots + r_0}_{i\ times}$ and $y = z + i \times r_0$ operations. The hidden ciphertext blocks z_i that result from the DES encryption (which operates on two 32-bit unsigned longs) are packed into the *unsigned long long* z_i for the subsequent modular 64-bit additions. Each packing operation, which would be avoided in a 64-bit implementation, requires a bitwise *or* and a shift.

The throughput of the CBC, XCBC$, CBC-MD5, CBC-UMAC-STD30,
CBC-HMAC-SHA1, and XCBC$-XOR modes implemented with DES is shown in Figure 1 for samples of both large and small messages. The percentage gain in the throughput performance of the XCBC$-XOR mode over that of the CBC-MD5, CBC-UMAC-STD30, and CBC-HMAC-SHA1 modes for these message samples is shown in Figure 2.

The results shown in these figures indicate that, in unoptimized software implementations,

- a substantial overall throughput improvement can be expected. For small messages (i.e., between 1

[5] Note that traditional CBC modes require the use of secret initialization vectors that are protected from arbitrary modification, and the most common way of satisfying both requirements is to use (pseudo) random initialization vectors. For this reason, the generation of the initial per-message random number is considered to be a common overhead to both the new and the traditional CBC modes. As shown above, the stateful XCBC mode, however, requires only that a separate random number be generated per key, not per message, thereby eliminating much of this common overhead of stateless modes. The alternative of generating and cacheing values of r_0 as the system runs and ahead of their actual use may also help decrease the overhead of the stateless XCBC mode.

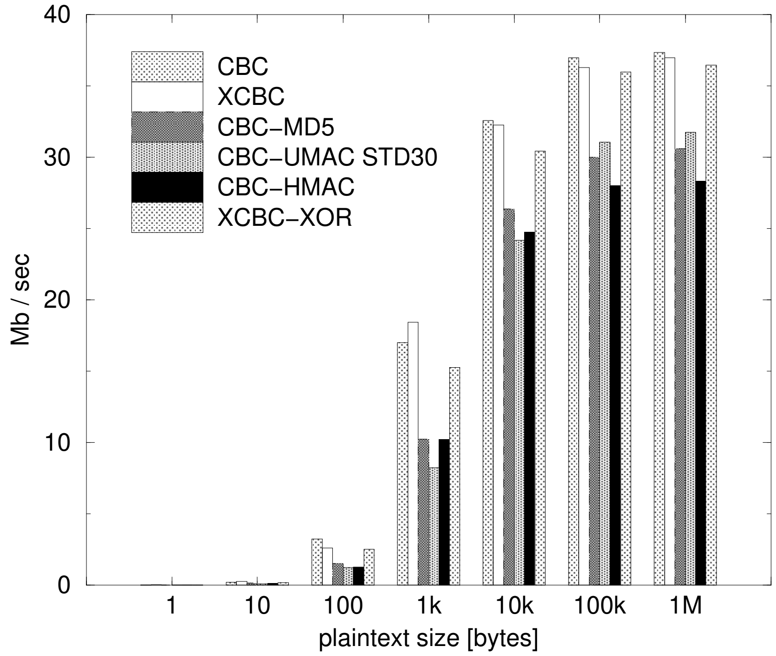

Figure 1: Throughput of the CBC, XCBC\$, CBC-MD5, CBC-UMAC-STD30, CBC-HMAC-SHA1, and XCBC\$-XOR encryption modes implemented with DES for message sizes of 1 B – 1 MB.

Byte and 1 KB length), we can expect about $15-65\%$ improvement for XCBC-XOR vs. CBC-MD5, about $78-113\%$ for XCBC-XOR vs. CBC-UMAC-STD30, and about $44-99\%$ for XCBC-XOR vs. CBC-HMAC-SHA1. For large messages (i.e., between 10 KB and 1MB length), we can expect about $15-20\%$ improvement for XCBC-XOR vs. CBC-MD5, about $15-25\%$ for XCBC-XOR vs. CBC-UMAC-STD30, and about $23-29\%$ for XCBC-XOR vs. CBC-HMAC-SHA1. In general, we expect higher performance improvement for small messages than for large ones because, for small messages, the performance of the MD5 hash function (and that of most hash functions), of UMAC-STD30 and HMAC-SHA1 is closer to that of DES than for large messages. Hence, our use of the function $g(x) = z_0 \oplus x_1 \oplus \cdots \oplus x_n$ improves a much larger fraction of the overall throughput of encrypted messages.

- throughput measurements for small-size messages shown in Figure 1 are susceptible to a significant margin of error caused by the inability to offset operating system effects over a fairly short run-time for each test for such messages. For example, for 1 KB messages, the throughput of XCBC\$ appears to be higher than that of CBC by about 8%. Nevertheless, the performance illustrated in Figure 1 appears to be consistent with individual MD5 and UMAC-STD30 measurements. For example, measurements reported for UMAC-STD30 [8] show that it reaches peak speeds for messages between 80 KB and 128 KB, whereas Figure 1 indicates that the UMAC-STD30 reaches close-to-peak performance at 100 KB. Also, Figure 1 shows that, for 10 KB messages, UMAC-STD30 is within 22.2% of the speed measured at 100 KB, which appears to be consistent with the measurements reported for UMAC-STD30.

- the clear performance bottleneck is that of the DES-CBC and underlying DES block encryption. Figure 1 shows that the performance differences between the DES-CBC, DES-XCBC\$, and DES-XCBC\$-XOR are almost imperceptible for mid-size and large messages. Given the advantage of using the function $g(x) = z_0 \oplus x_1 \oplus \cdots \oplus x_n$ over that of using $g(x) = $ MD5 or any other hash function

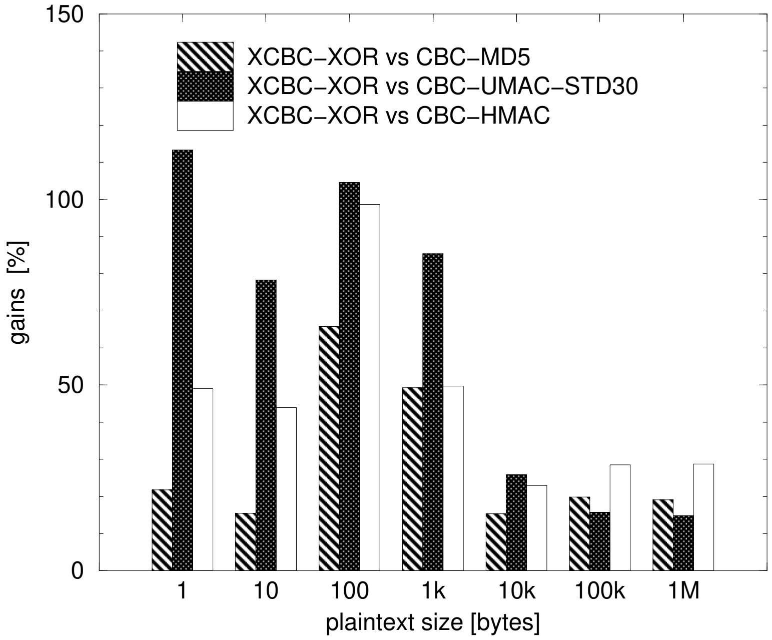

Figure 2: Percentage gains of the DES-XCBC$-XOR mode over the CBC-MD5, CBC-UMAC-STD30, and CBC-HMAC-SHA1 modes for message sizes of 1 B – 1 MB.

or MAC in XCBC encryption, we expect that the gain in the performance of the XCBC$-XOR over that of CBC-MD5 (or any other CBC-hash-function mode), CBC-UMAC-STD30, or CBC-HMAC-SHA1 to be even more pronounced for fast block encryption functions where the UMAC and MD5 (or any other hash function) would represent a higher fraction of the CBC-HMAC-SHA1, CBC-UMAC-STD30, and CBC-MD5 (or CBC-any-hash-function) cost.

We also expect that further improvements can be derived from an assembly language implementation where optimal register allocation can be performed for both the block encryption functions and the XCBC modes.

It should be noted that the implementation of the XCBC modes can be performed in software, hardware, or software with hardware support. Implementations can be in general-purpose computers or in dedicated hardware devices and software. The simplicity of the XCBC modes suggests that substantial cost-performance improvement can be expected when they are implemented in hardware. For example, DES hardware implementation reached 1.6 Gbp whereas HMAC-SHA-1 hardware implementation has reached only about half that speed. (This seems to confirm early predictions that the speed of hash functions and MACs based on them does not scale in hardware implementations as well as that of block encryption functions [31, 7]). Thus, we can expect performance speedups of about $100 - 200\%$ over current hardware implementation modes for message encryption and authentication. Of particular interest in this area are implementations of the XCBC modes on low-power and/or low-cost devices.

Acknowledgments

We thank David Wagner for pointing out an oversight in an earlier version of Theorem 2, Tal Malkin for her thoughtful comments and suggestions, Omer Horvitz and Radostina Koleva for their careful reading of this paper.

References

[1] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption," Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, 1997, (394-403). A full version of this paper is available at *http://www-cse.ucsd.edu/users/mihir.*

[2] M. Bellare, J. Killian, and P. Rogaway, "The security of cipher block chaining", *Advances in Cryptology-CRYPTO '94* (LNCS 839), 341-358, 1995.

[3] M. Bellare, R. Guerin, and P.Rogaway, "XOR MACs: New methods for message authentication using finite pseudo-random functions", Advances in Cryptology- CRYPTO '95 (LNCS 963), 15-28, 1995. (Also U.S. Patent No. 5,757,913, May 1998, and U.S. Patent No. 5,673,318, Sept. 1997.)

[4] M. Bellare and C. Namprempre, "Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm," manuscript, May 26, 2000. *http://eprint.iacr.org/2000.025.ps.*

[5] M. Bellare and P. Rogaway, "Block Cipher Mode of Operation for Secure, Length-Preserving Encryption," *U.S Patent No. 5,673,319,* September, 1997.

[6] M. Bellare and P. Rogaway, "On the construction of variable-input-length ciphers," Proceedings of the 6th Workshop on Fast Software Encryption, L. Knudsen (Ed), Springer-Verlag, 1999.

[7] S.M. Bellovin, "Cryptography and the Internet," *Advances in Cryptology - CRYPTO '98* (LNCS 1462), 46-55, 1998.

[8] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast Message Authentication via Optimized Universal Hash Functions," *Advances in Cryptology - CRYPTO '99* (LNCS 1666), 216-233, 1999.

[9] C.M. Campbell, "Design and Specification of Cryptographic Capabilities," in *Computer Security and the Data Encryption Standard*, (D.K. Brandstad (ed.)) National Bureau of Standards Special Publications 500-27, U.S. Department of Commerce, February 1978, pp. 54-66.

[10] Open Software Foundation, "OSF - Distributed Computing Environment (DCE), Remote Procedure Call Mechanisms," Code Snapshot 3, Release, 1.0, March 17, 1991.

[11] FIPS 81, "DES modes of operation", Federal Information Processing Standards Publication 81, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1980.

[12] V.D. Gligor and B. G. Lindsay,"Object Migration and Authentication," *IEEE-Transactions on Software Engineering*, SE-5 Vol. 6, November 1979. (Also IBM-Research Report RJ 2298 (3l04), August 1978.)

[13] V.D. Gligor, "Symmetric Encryption with Random Counters," University of Maryland, Computer Science Technical Report, CS-TR-3968, December 1998.

[14] V.D. Gligor, and P. Donescu, "Integrity-Aware PCBC Schemes," in Proc. of the 7th Int'l Workshop on *Security Protocols*, (B. Christianson, B.Crispo, and M. Roe (eds.)), Cambridge, U.K., LNCS 1796, April 2000.

[15] R.R. Juneman, S.M. Mathias, and C.H. Meyer, "Message Authentication with Manipulation Detection Codes," Proc. of the IEEE Symp. on Security and Privacy, Oakland, CA., April 1983, pp. 33-54.

[16] J. Katz and M. Yung, "Complete characterization of security notions for probabilistic private-key encryption," Proc. of the 32nd Annual Symp. on the Theory of Computing, ACM 2000.

[17] J. Katz and M. Yung, "Unforgeable Encryption and Adaptively Secure Modes of Operation," Proc. Fast Software Encryption 2000, B. Schneir (ed.) (to appear in Springer-Verlag, LNCS).

[18] D.E. Knuth, "The Art of Computer Programming - Volume 2: Seminumerical Algorithms," Addison-Wesley, 1981 (second edition), Chapter 3.

[19] J. T. Kohl, "The use of encryption in Kerberos for network authentication", *Advances in Cryptology-CRYPTO '89* (LNCS 435), 35-43, 1990.

[20] C.S. Jutla, "Encryption Modes with Almost Free Message Integrity," IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, manuscript, August 1, 2000. *http://eprint.iacr.org/2000/039.*

[21] C. H. Meyer and S. M. Matyas, *Cryptography; A New Dimension in Computer Data Security*, John Wiley & Sons, New York, 1982 (second printing).

[22] C. H. Meyer and S. M. Matyas, *Cryptography; A New Dimension in Computer Data Security*, John Wiley & Sons, New York, 1982 (third printing).

[23] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997.

[24] M. Naor and O. Reingold, "From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions from MACs," *Advances in Cryptology - CRYPTO '98* (LNCS 1462), 267-282, 1998.

[25] E. Petrank and C. Rackoff, "CBC MAC for Real-Time Data Sources," manuscript available at *http://philby.ucsd.edu/cryptolib.html*, 1997.

[26] RFC 1321, "The MD5 message-digest algorithm", Internet Request for Comments 1321, R. L. Rivest, April 1992 (presented at Rump Session of Crypto '91).

[27] RFC 1510, "The Kerberos network authentication service (V5)", Internet Request for Comments 1510, J. Kohl and B.C. Neuman, September 1993.

[28] P. Rogaway, "The Security of DESX," RSA Laboratories *Cryptobytes*, Vol. 2, No. 2, Summer 1996.

[29] S. G. Stubblebine and V. D. Gligor, "On message integrity in cryptographic protocols", Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, 85-104, 1992.

[30] SSLeay, available at *ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL*

[31] J. D. Touch, "Performance Analysis of MD5," Proceedings of ACM, SIGCOMM '95, 77-86, 1996.

[32] V.L. Voydock and S.T. Kent, "Security Mechanisms in high-level network protocols," *Computing Surveys*, 15(1983), 135-171.

[33] C. Weissman, "Question and Answer Session," in *Computer Security and the Data Encryption Standard*, (D.K. Brandstad (ed.)) National Bureau of Standards Special Publications 500-27, U.S. Department of Commerce, February 1978, pp. 121.

A Proofs

Proof [Security of the XCBC\$-XOR in a Message-Integrity Attack]

Notation: Throughout this proof, the superscripts of variables x^p, z^p, y^p, and r_0^p denote the plaintext, hidden ciphertext, ciphertext, and initial random value of a queried message $p, 1 \leq p \leq q_e$, whereas the (primed) variables x'^i, z'^i, y'^i, and $r_0'^i$ denote the plaintext, hidden ciphertext, ciphertext, and the initial random value of the i-th forged (i.e., unqueried) message, $1 \leq i \leq q_v$. The length of the plaintext of message p is denoted by $n_p = |x^p|$ and that of forgery y'^i by $n'^i = |x'^i|$ blocks. (These lengths do not include the last plaintext block that holds the value of the XOR function.)

To find an upper bound on the probability of an adversary's success we (1) define four types of events on which we condition the adversary's success, (2) express the upper bound in terms of the conditional probabilities obtained, and (3) compute upper bounds on these probabilities. Our choice and number of conditioning events is motivated exclusively by the need to obtain a (good) upper bound for the probability of the adversary's success. Undoubtedly, other events could be used for deriving alternate upper bounds.

To provide some intuition for the choice of conditioning events defined, we give examples of events that cause an adversary's success. (The reader can skip these examples without loss of continuity.)

Examples of Adversary's Success. A way for the adversary to find a forgery y' that passes the integrity check $g(x') = x'_{n+1}$, is to look for collisions in the input of f^{-1}, namely collisions of the (1) hidden ciphertext blocks generated during the decryption of a forgery, $z'_s, 1 \leq s \leq n+1$, and (2) initialization block y'_0 (i.e., block 0 of the forged ciphertext). These blocks could collide either with blocks $y_0^p, z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_i + 1$ obtained at encryption or among themselves. The following four examples illustrate why such collisions cause an adversary's success. Other such examples, and other ways to find forgeries, exist.

Example 1 – Collisions between blocks z'_s and z_k^p

Suppose that all hidden ciphertext blocks z'_s obtained during the decryption of forgery y' collide with some hidden ciphertext blocks z_k^p obtained at encryption. If this event occurs during forgery decryption, we declare pessimistically that the adversary is successful. Why is the adversary successful? Among the forgeries that make this event true, some will decrypt correctly with probability one. For example, if any two of the hidden ciphertext blocks between position 1 and n_p of a queried message p are swapped, the decryption of the resulting hidden ciphertext will pass the integrity check $g(x') = x'_{n+1}$ with probability one (viz., [23], Example 9.89, pp. 367-368, for a similar example). Thus, any forgery that generates such hidden ciphertext at decryption will pass this integrity check with probability one.

Why is our criterion for adversary's success based on such a collision event pessimistic? Among the forgeries that make this event true, some will decrypt correctly with negligible probability. These forgeries include truncations of the ciphertext of already queried messages. For truncations, the integrity check cannot pass with probability greater than $1/2^l$ (and for this reason we can focus on other types of forgeries for the rest of this proof).[6]

[6] Let the forged ciphertext y' be a truncation of ciphertext y^p obtained at encryption; i.e., $y'_s = y_s^p, \forall s, 0 \leq s \leq n'+1, |y'| = n'+1$ and $n' < n_p$, i.e., $n'+1 \leq n_p$. The condition $n'+1 \leq n_p$ (due to truncation) implies that all the plaintext blocks $x_1^p, \cdots, x_{n'+1}^p$ are constants. In this case, $z'_s = z_s^p, \forall s, 0 \leq s \leq n'+1$ and thus $x'_s = x_s^p, \forall s, 0 \leq s \leq n'+1$. The integrity check, $z_0^p \oplus x_1^p \oplus \cdots \oplus x_{n'}^p \oplus x_{n'+1}^p = 0$, is the exclusive-or of a random and uniformly distributed variable $z'_0 = f'(r'_0) = f'(r_0^p) = z_0^p$,

Example 2 – Collisions among the z'_s blocks

Suppose that two hidden ciphertext blocks z'_s and z'_t obtained during forgery decryption do not collide with any hidden ciphertext blocks obtained during encryption, but collide with each other. If this event occurs during forgery decryption, we declare pessimistically that the adversary is successful. Why is the adversary successful? Among the forgeries that make event true, some will decrypt correctly with probability one. For example, if any two identical blocks never seen among the hidden ciphertext blocks obtained at encryption are inserted into two adjacent positions between 1 and n_p of the hidden ciphertext of message p (i.e., $z'_s = z'_{s+1}, 1 \leq s < n_p - 1$), the decryption of the resulting hidden ciphertext will pass the integrity check $g(x') = x'_{n+1}$ with probability one (viz., [23], Example 9.89, pp. 367-368, for a similar example). Thus, any forgery that generates such hidden ciphertext blocks at decryption will pass this integrity check with probability one.

Why is our criterion for adversary's success based such a collision event pessimistic? Among the forgeries that make this event true, some will decrypt correctly with negligible probability. For example, consider forgeries that cause an odd number of identical hidden ciphertext blocks to be generated during decryption. Suppose these blocks have the following properties: (1) they do not collide with any hidden blocks obtained at encryption, (2) they do not collide with any initialization blocks $y_0^i, 1 \leq i \leq q_e$, obtained at encryption, (3) they do not collide with the initialization block y'_0 of the forgery, and (4) they appear between positions 1 and $n_p + 1$ of the hidden ciphertext of queried message p obtained at encryption. Forgeries that produce such blocks during decryption cannot pass the integrity check with probability greater than $1/2^l$. This is the case because the decryption of these identical hidden blocks produces random, uniformly distributed plaintext blocks that are independent of any other plaintext blocks in $g(x') = x'_{n+1}$ and can only cancel each other out in pairs under the exclusive-or operation.

The next two examples refer to collision events of the initialization block y'_0. These can lead to forgeries that satisfy the conditions of the events defined in Examples 1 and 2 above, and hence such collisions contribute to an adversary's success.

Example 3 – Collisions between blocks y'_0 and z^p_{k+1}

Suppose that, during the decryption of forgery y', block y'_0 collides with some hidden ciphertext block obtained during encryption. Let $y'_0 = z^p_{k+1}, 1 \leq p \leq q_e, 1 \leq k \leq n_p$. This means that the lower order bits of $r'_0 = f^{-1}(y'_0) = x^p_{k+1} \oplus z^p_k$ can be predicted (at least) to the same extent as those of z^p_k, since x^p_{k+1} is chosen. In (pessimistic) case the entire r'_0 is predicted, the adversary's forgeries can satisfy the collision events of Examples 1 and 2 above.

Example 4 – Collisions between blocks y_0^i and y_0^p

Suppose that an adversary finds a collision between the initialization blocks of two ciphertext messages i and p obtained at encryption, namely y_0^i and y^p, and chooses the initialization block of the forgery y' to be $y'_0 = y_0^i$. If the adversary can find such a collision event at encryption, the adversary can also find forgeries that satisfy the collision events of Example 1 at decryption. For example, the adversary can create a ciphertext message that has not been seen before (i.e., a forgery) by mixing the blocks of two ciphertext messages obtained at encryption whose initial ciphertext blocks collide; e.g., ciphertext block y_k^i of messages i replaces ciphertext $y_k^p \neq y_k^i$ of message p, where $y'_0 = y_0^i = y_0^p, i \neq p, n_i \leq n_p, 1 \leq i, p \leq q_e$,

where $f' \stackrel{R}{\leftarrow} R$, and constant plaintexts $x_1^p, \cdots, x^p_{n'+1}$. Hence, $Pr[z_0^p \oplus x_1^p \oplus \cdots \oplus x^p_{n'} \oplus x^p_{n'+1} = 0] = \frac{1}{2^l}$.

$1 \leq k \leq n_i$.

Conditioning Events. To compute an upper bound on the probability of successful forgery, we choose four conditioning events based on collisions in the input of f^{-1}. Intuition for the choice of events is provided by Examples 1 – 4 above.

For each verification query (or forgery) y'^i, $1 \leq i \leq q_v$, we define two types of collision events, C_i and D_i, that refer to the hidden ciphertext blocks $z_s'^i$ obtained during forgery decryption.

Event C_i includes all the instances when the hidden blocks $z_s'^i$ of forgery y'^i collide either with initialization blocks y_0^p or with some hidden ciphertext blocks z_k^p generated during encryption, where $1 \leq p \leq q_e, 1 \leq k \leq n_p + 1$. To define event C_i formally, let S be the the union of all the y_0^p blocks and all the hidden ciphertext blocks z_k^p produced at encryption:

$$S = \{y_0^p, 1 \leq p \leq q_e\} \cup \{z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_p + 1\}.$$

Also let Z_i be the collection of hidden ciphertext blocks z'^i generated during the decryption of the arbitrary forgery $y'^i, 1 \leq i \leq q_v$, that do not collide with blocks of S:

$$Z_i = \{z_s'^i, 1 \leq s \leq n_i' + 1, z_s'^i \notin S\}.$$

Hence, event C_i (*Collision*) is defined by:

$$C_i : Z_i = \emptyset;$$

i.e., Z_i is empty; or, equivalently, $C_i : Z_i \subseteq S$.

The second type of collision event defined for the arbitrary forgery $y'^i, 1 \leq i \leq q_v$, refers to collisions among blocks $y_0'^i, z_s'^i, 1 \leq s \leq n_i' + 1$ where $z_s'^i \in Z_i$, and is denoted by $\overline{D_i}$ (*not distinct*) below. This event is defined in terms of its complementary event D_i (*distinct*), which states that there is at least a hidden block $z_s'^i \in Z_i$ that does not collide with any other hidden block $z_t'^i \in Z_i$ or with $y_0'^i$.[7] It is clear that this definition makes sense only when $Z_i \neq \emptyset$. Formally, if $Z_i \neq \emptyset$,

$$D_i : \exists z_s'^i \in Z_i, 1 \leq s \leq n_i' + 1 : z_s'^i \neq z_t'^i, \forall z_t'^i \in Z_i, t \neq s, 1 \leq t \leq n_i' + 1 \text{ and } z_s'^i \neq y_0'^i.$$

The third type of collision event for the arbitrary forgery $y'^i, 1 \leq i \leq q_v$, which is denoted by I_i below, includes all the instances when the initialization block $y_0'^i$ collides with some hidden ciphertext blocks generated during encryption (i.e., $z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_i + 1$). Formally, event I_i is defined by:

$$I_i : y_0'^i \in S - \{y_0^p, 1 \leq p \leq q_e\},$$

or, equivalently,

$$I_i : y_0'^i \in \{z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_p + 1\},$$

The fourth type of collision event, denoted by E below, defines collisions among the initialization blocks (i.e., block 0 of the ciphertext) generated at encryption. (Hence, this collision event is independent of the forgery y'^i.) Formally, this event is defined as

$$E : y_0^i = y_0^p,$$

where $i \neq p, 1 \leq i, p \leq q_e$.

[7] Recall that hidden ciphertext blocks $z_s'^i, z_t'^i \in Z_i$ do not collide with any z_k^p or with any y_0^p obtained during encryption, where $1 \leq p \leq q_e, 1 \leq k \leq n_p + 1$.

Note 1: Other events than the four defined above could cause an adversary's forgery y'^i to pass the integrity check $g(x'^i) = x'^i_{n_i+1}$. However, Claim 1 below makes it clear that the success of such a forgery could only occur with probability no greater than $1/2^l$.

Note 2: Another collision event in the input of f^{-1}, $y'^i_0 = y^p_0, 1 \le i \le q_v, 1 \le p \le q_e$, can be caused simply be the adversary's choice of the initial forgery block. Unlike the four events defined above (and illustrated by Examples 1 – 4), the occurrence of this collision event cannot cause an adversary's success in the absence of other collision events. Nevertheless, the occurrence of this event is accounted for in the proof; viz., Proof of Claim 3 below.

Upper bound on the Probability of Successful Forgery. Let R be the set of all functions $\{0,1\}^l \to \{0,1\}^l$, and $f \stackrel{\mathcal{R}}{\leftarrow} R$ denotes the random selection of f from R. For the balance of this proof, we use the result of Fact 1 below (whose standard proof can be found at the end of this appendix).

Fact 1

$$Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[\text{Succ}] \le \epsilon + Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[\text{Succ}].$$

Fact 1 reduces the problem to finding an upper bound for $Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[\text{Succ}]$. Unless we state otherwise, assume that $f \stackrel{\mathcal{R}}{\leftarrow} R$ (and drop this subscript from $Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[\text{Succ}]$.)

To compute an upper bound for the probability of successful forgery, $Pr[\text{Succ}]$, we condition on event E first, since this event does not depend on the forgery y'^i. Using standard conditioning, we obtain

$$Pr[\text{Succ}] \le Pr[E] + Pr[\text{Succ} \mid \overline{E}].$$

Since event E is equivalent to the event that at least a collision happens when q_e balls are thrown at random in 2^l buckets [3],

$$Pr[E] \le \frac{q_e^2}{2^l}.$$

To find an upper bound for $Pr[\text{Succ} \mid \overline{E}]$, we use the definition of adversary's success (viz., the attack definition), which states that at least one forgery (and verification query) y'^i succeeds; i.e., there exists an index $i, 1 \le i \le q_v$ such that $g(x'^i) = x'^i_{n'_i+1}$. Hence, by union bound,

$$Pr[\text{Succ} \mid \overline{E}] \le \sum_{i=1}^{q_v} Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E}].$$

To find an upper bound for the probability of decrypting a single, arbitrary (non-truncation) forgery y'^i correctly given $\overline{E}$, namely for $Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E}]$, we condition on event (C_i or $\overline{D_i}$). Using the total probability formula we obtain:

$$\begin{aligned} Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E}] \quad = \quad & Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E} \text{ and } (C_i \text{ or } \overline{D_i})] Pr[C_i \text{ or } \overline{D_i} \mid \overline{E}] + \\ & Pr[g(x'^i) = x'^i_{n'^i+1} \mid \overline{E} \text{ and } (\overline{C_i} \text{ and } D_i)] Pr[\overline{C_i} \text{ and } D_i \mid \overline{E}]. \end{aligned}$$

Hence,[8]

$$Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E}] \le Pr[C_i \text{ or } \overline{D_i} \mid \overline{E}] + Pr[g(x'^i) = x'^i_{n'^i+1} \mid \overline{E} \text{ and } \overline{C_i} \text{ and } D_i].$$

[8]This also follows from our pessimistic assumption that if event (C_i or $\overline{D_i}$) is true, then the adversary has broken integrity.

However, both event C_i and event $\overline{D_i}$ depend on the event I_i (viz., Example 3 above). Hence, to compute $Pr[C_i \text{ or } \overline{D_i} \mid \overline{E}]$ we condition on event I_i and, using the total probability formula, we obtain:

$$\begin{aligned} Pr[C_i \text{ or } \overline{D_i} \mid \overline{E}] &= Pr[C_i \text{ or } \overline{D_i} \mid \overline{E} \text{ and } I_i] Pr[I_i \mid \overline{E}] + Pr[C_i \text{ or } \overline{D_i} \mid \overline{E} \text{ and } \overline{I_i}] Pr[\overline{I_i} \mid \overline{E}] \\ &\leq Pr[I_i \mid \overline{E}] + Pr[C_i \text{ or } \overline{D_i} \mid \overline{E} \text{ and } \overline{I_i}]. \end{aligned}$$

Furthermore,

$$\begin{aligned} Pr[C_i \text{ or } \overline{D_i} \mid \overline{E} \text{ and } \overline{I_i}] &= Pr[C_i \text{ or } \overline{D_i} \mid \overline{C_i} \text{ and } \overline{E} \text{ and } \overline{I_i}] Pr[\overline{C_i} \mid \overline{E} \text{ and } \overline{I_i}] \\ &\quad + Pr[C_i \text{ or } \overline{D_i} \mid C_i \text{ and } \overline{E} \text{ and } \overline{I_i}] Pr[C_i \mid \overline{E} \text{ and } \overline{I_i}] \\ &\leq Pr[C_i \text{ or } \overline{D_i} \mid \overline{C_i} \text{ and } \overline{E} \text{ and } \overline{I_i}] + Pr[C_i \mid \overline{E} \text{ and } \overline{I_i}] \\ &= Pr[C_i \mid \overline{E} \text{ and } \overline{I_i}] + Pr[\overline{D_i} \mid \overline{C_i} \text{ and } \overline{E} \text{ and } \overline{I_i}], \end{aligned}$$

since event $[C_i \text{ or } \overline{D_i} \mid \overline{C_i} \text{ and } \overline{E} \text{ and } \overline{I_i}]$ is equivalent to event $[\overline{D_i} \mid \overline{C_i} \text{ and } \overline{E} \text{ and } \overline{I_i}]$.

Combining the results of the last three inequalities, we obtain:

$$\begin{aligned} Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E}] &\leq Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E} \text{ and } \overline{C_i} \text{ and } D_i] + \\ &\quad Pr[I_i \mid \overline{E}] + Pr[C_i | \overline{E} \text{ and } \overline{I_i}]. + Pr[\overline{D_i} \mid \overline{C_i} \text{ and } \overline{E} \text{ and } \overline{I_i}] \end{aligned}$$

The probabilities that appear at the right side of this inequality are bounded as shown in the following four claims whose proofs are included below. (Note again that forgeries based on truncations of ciphertext messages obtained at encryption are *not* included in any of the claims below. All these claims refer to a single, arbitrary (non-truncation) forgery $y'^i, 1 \leq i \leq q_v$.)

Claim 1

$$Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E} \text{ and } \overline{C_i} \text{ and } D_i] \leq \frac{1}{2^l}.$$

Claim 2

$$Pr[I_i \mid \overline{E}] \leq \frac{1}{2^l} \frac{\mu_e}{2l} \left(\log_2 \frac{\mu_e}{l} + 3 \right).$$

Claim 3

$$Pr[C_i | \overline{E} \text{ and } \overline{I_i}] \leq \frac{(n'_i + 1) q_e}{2^l} + \frac{1}{2^l} \frac{\mu_e}{2l} \left(\log_2 \frac{\mu_e}{l} + 3 \right).$$

Claim 4

$$Pr[\overline{D_i} \mid \overline{C_i} \text{ and } \overline{E} \text{ and } \overline{I_i}] \leq \frac{2n'_i + 1}{2^l}.$$

Note that if the maximum length m of the encrypted messages is known, the $\log_2 \frac{\mu_e}{l}$ term of Claims 2 and 3 can be replaced with $\log_2 m$.

By Claims 1–4, the probability of success given $\overline{E}$ for a single, arbitrary (non-truncation) forgery is

$$\begin{aligned} Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E}] &\leq \frac{1}{2^l} + \frac{(n'_i + 1) q_e}{2^l} + \frac{1}{2^l} \left(\frac{\mu_e}{l} \log_2 \frac{\mu_e}{l} + \frac{3\mu_e}{l} \right) + \frac{2n'_i + 1}{2^l} \\ &= \frac{(n'_i + 1)(q_e + 2)}{2^l} + \frac{1}{2^l} \left(\frac{\mu_e}{l} \log_2 \frac{\mu_e}{l} + \frac{3\mu_e}{l} \right). \end{aligned}$$

Hence, the probability of adversary success when he has up to q_v verification queries totaling at most μ_v bits and using up to t_v time is bounded by

$$\begin{aligned} Pr[\text{Succ}] &\leq Pr[E] + \sum_{i=1}^{q_v} Pr[g(x'^i) = x'^i_{n'_i+1} \mid \overline{E}] \\ &\leq \frac{q_e^2}{2^l} + \sum_{i=1}^{q_v} \left(\frac{(n'_i+1)(q_e+2)}{2^l} + \frac{1}{2^l} \left(\frac{\mu_e}{l} \log_2 \frac{\mu_e}{l} + \frac{3\mu_e}{l} \right) \right) \\ &\leq \frac{q_e^2}{2^l} + \frac{\mu_v(q_e+2)}{l 2^l} + \frac{q_v}{2^l} \left(\frac{\mu_e}{l} \log_2 \frac{\mu_e}{l} + \frac{3\mu_e}{l} \right) \end{aligned}$$

because $\sum_{i=1}^{q_v} (n'_i + 1) \leq \frac{\mu_v}{l}$.

Furthermore, by using Fact 1, the probability of adversary's success when $f \xleftarrow{\mathcal{R}} F$ is bounded by:

$$Pr_{f \xleftarrow{\mathcal{R}} F}[\text{Succ}] \leq \epsilon + \frac{q_e^2}{2^l} + \frac{\mu_v(q_e+2)}{l 2^l} + \frac{q_v}{2^l} \left(\frac{\mu_e}{l} \log_2 \frac{\mu_e}{l} + \frac{3\mu_e}{l} \right).$$

Also, if the maximum length m of the encrypted messages is known, the last term of the above bounds can be replaced with $\frac{q_v}{2^l} \left(\frac{\mu_e}{l} \log_2 m + \frac{3\mu_e}{l} \right)$.

The parameters of the attack are bounded as follows: $q_e \leq q'$, since the scheme is also supposed to be chosen-plaintext secure, $t_e + t_v \leq t$, and $\mu'' = \mu_e + \mu_v \leq ql$. The forgery verification parameters q_v, μ_v, t_v can be chosen within the constraints of these bounds and the desired $Pr_{f \xleftarrow{\mathcal{R}} F}[Succ]$. $\square$

Proofs of Claims 1–4

Notation: Recall that Claims 1 – 4 above refer to a *single*, arbitrary (non-truncation) forgery $y'^i, 1 \leq i \leq q_v$. Hence, to simplify notation in the proof of these claims, we drop the forgery index i from the events D_i, C_i, I_i, and simply use D, C, I for these events. We also drop the forgery index i from the collection Z_i and use Z instead. Furthermore, we drop the prime and forgery index i from the ciphertext y'^i, hidden ciphertext, z'^i, plaintext x'^i, r'^i_0, and the length n'_i. Hence, when we refer to the (single) forgery, we use the variables y, for forgery ciphertext, x for forgery plaintext, z for the hidden blocks of forgery y, y_0 for the initialization block of forgery y (and r_0 for the decryption of the initialization block y_0), and n for the length of x. Superscripts continue to identify encryption queries. In the proof of Claims 1 – 4, we use the notation $Pr_A[\ .\ ] = Pr[\ .\ |A]$, where A is an arbitrary event.

Proof of Claim 1

If $\overline{C}$ is true, then Z is not empty. For any $z_s \in Z$,

$$x_s = f^{-1}(z_s) \oplus z_{s-1}$$

Since z_s does not collide with any hidden blocks obtained at encryption, and event ($\overline{C}$ and D) is true (i.e., there is at least one hidden block $z_s \in Z$ by event $\overline{C}$ that does not collide with another hidden ciphertext block $z_t \in Z, s \neq t$ or with y_0 by event D), then $f^{-1}(z_s)$ is uniformly distributed and independent of anything else; i.e., independent of any other $f^{-1}(z_k), z_k \in Z$, $k \neq s$, and independent of any $z_k, 0 \leq k \leq$

$n+1$. Hence, the corresponding plaintext block x_s is uniformly distributed and independent of anything else. Thus,

$$g(x) \oplus x_{n+1} = z_0 \oplus x_1 \oplus \cdots \oplus x_n \oplus x_{n+1}$$

is random and uniformly distributed, and hence:

$$Pr[g(x) \oplus x_{n+1} = 0 \mid \overline{E} \text{ and } \overline{C} \text{ and } D] = Pr[g(x) = x_{n+1} \mid \overline{E} \text{ and } \overline{C} \text{ and } D] \leq \frac{1}{2^l}.$$

□

In the proofs of Claims 2 – 4, we use the following three facts, whose proofs can be found at the end of this appendix.

Fact 2
For any $1 \leq i \leq 2^l - 1$, let m be defined by $i = d \times 2^m$, where d is odd. If r_0 is random and uniformly distributed, then for any constant a,

$$Pr[i \times r_0 = a] \leq \frac{1}{2^{l-m}}.$$

Fact 3
For any $N > 1$, let m be defined by $a = d \times 2^m$, where $1 \leq a \leq N-1$ and d is odd. Then

$$\sum_{a=1}^{N-1} 2^m \leq \frac{N-1}{2}(\log_2(N-1) + 3).$$

Fact 4
If for any $p, 1 \leq p \leq q_e, n_p > 0$, and if $\sum_{p=1}^{q_e}(n_p + 1) \leq \frac{\mu_e}{l}$, then,

$$\sum_{p=1}^{q_e}(n_p + 1)\log_2(n_p + 1) \leq \frac{\mu_e}{l}\log_2\frac{\mu_e}{l};$$

and, further, if $m = \max(n_p + 1)$, then

$$\sum_{p=1}^{q_e}(n_p + 1)\log_2(n_p + 1) \leq \frac{\mu_e}{l}\log_2 m.$$

Proof of Claim 2

Event $I : y_0 \in S - \{y_0^p, 1 \leq p \leq q_e\} = \{z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_p + 1\}$ is equivalent to the union of all possible events $y_0 = z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_p + 1$. Hence, by union bound,

$$Pr[I \mid \overline{E}] \leq \sum_{p=1}^{q_e}\sum_{k=1}^{n_p+1} Pr[y_0 = z_k^p \mid \overline{E}].$$

We determine an upper bound for $Pr[y_0 = z_k^p \mid \overline{E}]$ based on

$$y_0 = z_k^p \;\Leftrightarrow\; y_0 = y_k^p - k \times r_0^p \;\Leftrightarrow\; k \times r_0^p = y_k^p - y_0.$$

In this expression, r_0^p is random and uniformly distributed, and from the definition of event E, if $\overline{E}$ is true, then r_0^p is random and uniformly distributed. Hence, since $y_k^p - y_0$ is a known constant, by Fact 2,

$$Pr[y_0 = z_k^p \mid \overline{E}] = Pr[k \times r_0^p = y_k^p - y_0 \mid \overline{E}] \leq \frac{1}{2^{l-m}},$$

where the exponent m is defined by $k = d \times 2^m$ and d is odd. Hence, for each $p, 1 \leq p \leq q_e$, from this and Fact 3 with $N - 1 = n_p + 1$ and $a = k$,

$$\sum_{k=1}^{n_p+1} Pr[y_0 = z_k^p \mid \overline{E}] \leq \frac{1}{2^l} \sum_{k=1}^{n_p+1} 2^m \leq \frac{1}{2^l} \frac{n_p+1}{2} (\log_2(n_p+1) + 3).$$

Since $\sum_{p=1}^{q_e} (n_p + 1) \leq \frac{\mu_e}{l}$ by the definition of $n + p$ and of the attack, we obtain

$$Pr[I \mid \overline{E}] \quad \leq \quad \sum_{p=1}^{q_e} \sum_{k=1}^{n_p+1} Pr[y_0 = z_k^p \mid \overline{E}] \leq \frac{1}{2^l} \sum_{p=1}^{q_e} \frac{n_p+1}{2} (\log_2(n_p+1) + 3) \leq \frac{1}{2^l} \frac{\mu_e}{2l} \left(\log_2 \frac{\mu_e}{l} + 3 \right),$$

by Fact 4. Further, if $m = \max(n_p + 1)$, then $Pr[I \mid \overline{E}] \leq \frac{1}{2^l} \frac{\mu_e}{2l} (\log_2 m + 3)$, also by Fact 4. □

Proof of Claim 3

Below we use the notation that $Pr_A[\ .\ ] = Pr[\ .\ |A]$, where A is an arbitrary event.

C is equivalent to the event that every hidden ciphertext block obtained during decryption is found among the hidden ciphertext blocks obtained during encryption or among the y_0^p blocks obtained at encryption. This implies that *for any* $s, 1 \leq s \leq n+1$: $Pr_{\overline{I} \text{ and } \overline{E}}[C] \leq Pr_{\overline{I} \text{ and } \overline{E}}[z_s \in S]$ by union bound. Since, $S = \{y_0^p, 1 \leq p \leq q_e\} \cup \{z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_p + 1\}$, it follows that, by union bound,

$$\begin{aligned} Pr_{\overline{I} \text{ and } \overline{E}}[z_s \in S] \quad &\leq \quad Pr_{\overline{I} \text{ and } \overline{E}}[z_s \in \{y_0^p, 1 \leq p \leq q_e\}] \\ &+ \quad Pr_{\overline{I} \text{ and } \overline{E}}[z_s \in \{z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_p + 1\}]. \end{aligned}$$

For the first term, for any $s, 1 \leq s \leq n+1$, the event $z_s \in \{y_0^p, 1 \leq p \leq q_e\}$ is the union of all collision events $z_s = y_0^p, 1 \leq p \leq q_e$. Hence,

$$Pr_{\overline{I} \text{ and } \overline{E}}[z_s \in \{y_0^p, 1 \leq p \leq q_e\}] \leq \sum_{p=1}^{q_e} Pr_{\overline{I} \text{ and } \overline{E}}[z_s = y_0^p].$$

But $z_s = y_s - s \times r_0$ by the scheme definition, and hence $s \times r_0 = y_s - y_0^p$. To compute $Pr_{\overline{I} \text{ and } \overline{E}}[s \times r_0 = y_s - y_0^p]$, we use the following claim, whose proof can be found at the end of this appendix:

Claim 3.1
Let $y_0^p y_1^p \cdots y_{n_p+1}^p$ be a queried message, and $y = y_0 y_1 \cdots y_{n+1}$ be a forged ciphertext. If event $\overline{I}$ is true, then r_0 is random and uniformly distributed. Furthermore, if $r_0 \neq r_0^p$, then r_0 is also independent of r_0^p.

Since event $\overline{I}$ is true, it follows that r_0 is random and uniformly distributed (by Claim 3.1 above). Also, event $\overline{I}$ and $\overline{E}$ implies that r_0 is random and uniformly distributed by the definition of event E. Hence, by Fact 2,

$$Pr_{\overline{I} \text{ and } \overline{E}}[s \times r_0 = y_s - y_0^p] \leq \frac{1}{2^{l-m}},$$

where m is defined by $s = d \times 2^m$ and d is odd. Furthermore, $m \le \log_2 s \le \log_2(n+1)$, since $s \le n+1$. Hence, $2^m \le n+1$, and

$$Pr_{\overline{I} \text{ and } \overline{E}}[s \times r_0 = y_s - y_0^p] \le \frac{n+1}{2^l}.$$

Hence, for any $s, 1 \le s \le n+1$:

$$Pr_{\overline{I} \text{ and } \overline{E}}[z_s \in \{y_0^p, 1 \le p \le q_e\}] \le \sum_{p=1}^{q_e} \frac{n+1}{2^l} = \frac{(n+1)q_e}{2^l}.$$

To compute an upper bound for the second term, namely on $Pr_{\overline{I} \text{ and } \overline{E}}[z_s \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}]$, we are free to choose a hidden ciphertext block at index j of forgery y, namely z_j, and then we only need to show that $Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}]$, is bounded. (This is the case because the bound must be true *for any* $s, 1 \le s \le n+1$.)

Thus, the balance of the proof of Claim 3 consists of two parts. In the first part, we partition the space of forgeries that are not truncations into three complementary types and choose a z_j (and hence, index j) for each type. In the second part, we find an upper bound for the probability $Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}]$ for each of the chosen z_j's. Hence, the maximum of these three upper bounds represents the upper bound for $Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}]$ for all forgeries that are not truncations.

Part 1. Finding index j depends on the type of forgery. A forgery can be such that a ciphertext obtained at encryption is the prefix of the forgery; we call this the *prefix* case. The complementary case for the prefix case, which we call *non-prefix*, includes two separate subcases, namely when y_0 is different from any y_0^i of any ciphertext obtained at encryption, or when there is an index i such that $y_0 = y_0^i$. Hence, in the latter case, there must be at least a block in the forged ciphertext y that is different from the corresponding block of the ciphertext of a queried message i, namely y^i. Further, the length of the forged ciphertext y, denoted by n, may be different from the length of the message plaintext defined by n_i.

This partition of forgery types shows that a forged ciphertext $y = y_0 y_1 \cdots y_{n+1}$, which is not a truncation, can be in one of the following three complementary types:
(a) $\exists i, 1 \le i \le q_e : n > n_i, \forall k, 0 \le k \le n_i + 1 : y_k = y_k^i$; i.e., the forged ciphertext is an extension of the ciphertext y^i (the prefix case). The non-prefix case consists of the following two forgery types:
(b1) $y_0 \ne y_0^i, \forall i, 1 \le i \le q_e$; i.e., the forged ciphertext and all queried-message ciphertexts differ in the first block.
(b2) $\exists i, 1 \le i \le q_e : y_0 = y_0^i, \exists k, 1 \le k \le \min(n_i + 1, n+1) : y_k \ne y_k^i$; i.e., the forged ciphertext is obtained by modifying a queried message ciphertext starting with some block between the second and last block of that queried-message ciphertext. In this case, let j be the smallest index such that $y_j \ne y_j^i$ (i.e., $\forall k, 0 \le k \le j-1 : y_k = y_k^i$).

Let us choose index j (and hence z_j) as follows. For forgeries of type (a), $j = n_i + 2$ (or $j > n_i + 1$); for forgeries of type (b1), $j = 1$; and for forgeries of type (b2), j is the smallest index such that $y_j \ne y_j^i, 1 \le j \le \min\{n_i + 1, n+1\}$. In all cases $j \ge 1$, and hence, the chosen ciphertext block z_j is well defined.

Part 2. For the index j chosen in Part 1, we find an upper bound for $Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}]$. Event $z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}$ is the union of all possible events

$z_j = z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_p + 1$. Hence, union bound leads to:

$$Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \leq p \leq q_e, 1 \leq k \leq n_p + 1\}] \leq \sum_{p=1}^{q_e} \sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p].$$

Now we find an upper bound for $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p]$ for each of the three forgery types. In determining this upper bound, we use the following claim, whose proof can be found at the end of this appendix:

Claim 3.2
Let $z_k^p, 1 \leq p \leq q_e$, be the hidden ciphertext blocks generated at the encryption of a queried message $y_0^p y_1^p \cdots y_{n_p+1}^p$, and z_j be the chosen hidden ciphertext block generated during the decryption of forgery $y = y_0, y_1, \cdots y_{n+1}$. Then $\forall k, 1 \leq k \leq n_p + 1$,

$$Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \leq \frac{1}{2^{l-m}},$$

where
(a) if $y_0 \neq y_0^p$, then $m = \min(m_1, m_2)$, with m_1 and m_2 being defined by $j = d_1 \times 2^{m_1}$, $k = d_2 \times 2^{m_2}$, where d_1, d_2 are odd; and
(b) if $y_0 = y_0^p$, where m is defined by $k - j = d \times 2^m$ if $k > j$, or by $j - k = d \times 2^m$ if $j < k$, and d is odd.

Claim 3.2 provides upper bounds for $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p]$, where p, k are arbitrary values that satisfy the hypotheses of parts (a) or (b) and z_j is the chosen hidden ciphertext block defined in Part 1. These hypotheses are verified for the chosen j of each forgery type as shown below.

Upper bound for forgeries of type (a).
Let the ciphertext of queried message i be the prefix of forgery y. To find the upper bound in this case, we partition the sum $\sum_{p=1}^{q_e} \sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p]$ into two sums, for $p \neq i$ and $p = i$, respectively. For $p \neq i$, we use Claim 3.2(a), and for $p = i$ we use Claim 3.2(b), to find an upper bound for $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p]$. Then we find individual upper bounds for each of these two sums, and add these upper bounds.

$$\sum_{p=1}^{q_e} \sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] = \sum_{p=1, p \neq i}^{q_e} \sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] + \sum_{k=1}^{n_i+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i].$$

For the first sum, note that $p \neq i$, and recall that for forgeries of type (a) $y_0 = y_0^i$. Since $\overline{E}$ is true, $y_0 = y_0^i \neq y_0^p$. Hence, by Claim 3.2(a), $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \leq \frac{1}{2^{l-m}}$, where $m \leq m_2$ with m_2 being defined by $k = d_2 \times 2^{m_2}$ and d_2 is odd. Thus,

$$\sum_{p=1, p \neq i}^{q_e} \sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \leq \frac{1}{2^l} \sum_{p=1, p \neq i}^{q_e} \sum_{k=1}^{n_p+1} 2^{m_2}.$$

But, by Fact 3 with $N - 1 = n_p + 1$ and $a = k$,

$$\sum_{k=1}^{n_p+1} 2^{m_2} \leq \frac{n_p + 1}{2}(\log_2(n_p + 1) + 3).$$

Hence,

$$\sum_{p=1, p \neq i}^{q_e} \sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \leq \frac{1}{2^l} \sum_{p=1, p \neq i}^{q_e} \frac{n_p + 1}{2}(\log_2(n_p + 1) + 3).$$

For the second sum, we note that $p = i$, which means that $y_0 = y_0^i = y_0^p$, and that $j = n_i + 2 > k, \forall k, 1 \le k \le n_i + 1$. Hence, by Claim 3.2(b) $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \le \frac{1}{2^{l-m}}$, where $j - k = d \times 2^m$ and d is odd. Since $j = n_i + 2$, in follows that $j - k = n_i + 1, \cdots, 1$, and thus,

$$\sum_{k=1}^{n_i+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \le \sum_{j-k=1}^{n_i+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \frac{1}{2^l} \sum_{j-k=1}^{n_i+1} 2^m.$$

But, by Fact 3 with $N - 1 = n_i + 1$ and $a = j - k$,

$$\sum_{j-k=1}^{n_i+1} 2^m \le \frac{n_i + 1}{2} (\log_2(n_i + 1) + 3),$$

and hence,

$$\sum_{k=1}^{n_i+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \le \frac{1}{2^l} \frac{n_i + 1}{2} (\log_2(n_i + 1) + 3).$$

Adding the two upper bounds, we obtain

$$\begin{aligned} \sum_{p=1}^{q_e} \sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] &\le \frac{1}{2^l} \frac{n_i + 1}{2} (\log_2(n_i + 1) + 3) + \frac{1}{2^l} \sum_{p=1, p \ne i}^{q_e} \frac{n_p + 1}{2} (\log_2(n_p + 1) + 3) \\ &= \frac{1}{2^l} \sum_{p=1}^{q_e} \frac{n_p + 1}{2} (\log_2(n_p + 1) + 3). \end{aligned}$$

Since $\sum_{p=1}^{q_e} (n_p + 1) \le \frac{\mu_e}{l}$, by Fact 4, it follows that

$$\begin{aligned} & Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}] \le \\ & \quad \sum_{p=1}^{q_e} \sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \le \frac{1}{2^l} \frac{\mu_e}{2l} \left(\log_2 \frac{\mu_e}{l} + 3 \right). \end{aligned}$$

Further, if $m = \max(n_p + 1)$, then $Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}] \le \frac{1}{2^l} \frac{\mu_e}{2l} (\log_2 m + 3)$, also by Fact 4.

Upper bound for forgeries of type (b1).
For this type of forgery, $y_0 \ne y_0^p, \forall p, 1 \le p \le q_e$. Hence, by Claim 3.2(a), $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \le \frac{1}{2^{l-m}}$, where $m \le m_2$ with m_2 being defined by $k = d_2 \times 2^{m_2}$ and d_2 is odd. By following the same derivation as that for forgeries of type (a), we obtain:

$$\begin{aligned} & Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}] \le \sum_{p=1}^{q_e} \sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \le \\ & \frac{1}{2^l} \sum_{p=1}^{q_e} \sum_{k=1}^{n_p+1} 2^{m_2} \le \frac{1}{2^l} \sum_{p=1}^{q_e} \frac{n_p + 1}{2} (\log_2(n_p + 1) + 3) \le \frac{1}{2^l} \frac{\mu_e}{2l} \left(\log_2 \frac{\mu_e}{l} + 3 \right). \end{aligned}$$

Also, if $m = \max(n_p + 1)$, then $Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}] \le \frac{1}{2^l} \frac{\mu_e}{2l} (\log_2 m + 3)$.

Upper bound for forgeries of type (b2).
Let the first $j - 1$ ciphertext blocks of queried message i provide the first $j - 1$ ciphertext blocks of forgery

y. To find the upper bound in this case, we partition the sum $\sum_{p=1}^{q_e}\sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p]$ into four terms, find individual upper bounds for each term, and then add these upper bounds. The first term is a sum taken for $p \neq i$ and in this case we use Claim 3.2(a) to find an upper bound for $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p]$. The last three terms are for the case $p = i$, and two of these terms are sums taken for $k < j$ and $k > j$, respectively. For these sums, we apply Claim 3.2(b) to find an upper bound for $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p]$. For the remaining term corresponding to $i = p$ and $k = j$, we show that the event $z_j = z_k^p$ is impossible.

$$\begin{aligned}\sum_{p=1}^{q_e}\sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \quad &= \quad \sum_{p=1,p\neq i}^{q_e}\sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] + \sum_{k=1}^{j-1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] + Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_j^i] + \\ &\quad \sum_{k=j+1}^{n_i+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i].\end{aligned}$$

For the first of the four terms above, we have the same bound as that of the first of the two sums in the case of forgeries of type (a) above, namely,

$$\sum_{p=1,p\neq i}^{q_e}\sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \leq \frac{1}{2^l}\sum_{p=1,p\neq i}^{q_e}\frac{n_p+1}{2}(\log_2(n_p+1)+3).$$

For the second term, namely $\sum_{k=1}^{j-1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i]$, we note that $i = p$, which means that $y_0 = y_0^i = y_0^p$, and $k < j$. Hence, by Claim 3.2(b), $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \leq \frac{1}{2^{l-m}}$, where $j - k = d \times 2^m$ and d is odd. Since $k = 1, \cdots, j-1$, it follows that $j - k = j-1, \cdots, 1$, and by Fact 3 with $N - 1 = j - 1$ and $a = j - k$,

$$\sum_{k=1}^{j-1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \quad = \quad \sum_{j-k=1}^{j-1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \leq \frac{1}{2^l}\sum_{j-k=1}^{j-1} 2^m \leq \frac{1}{2^l}\frac{j-1}{2}(\log_2(j-1)+3).$$

For the third term, $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_j^i] = 0$. This is the case because $z_j = z_j^i \;\Leftrightarrow\; y_j - j \times r_0 = y_j^i - j \times r_0^i$ and, since $y_0 = y_0^i \;\Leftrightarrow\; r_0 = r_0^i$, it follows that $z_j = z_j^i \;\Leftrightarrow\; y_j = y_j^i$, which is impossible by the definition of j. (Recall that for forgeries of type (b2), j is the smallest index such that $y_j \neq y_j^i, 1 \leq j \leq \min\{n_i+1, n+1\}$.)

For the fourth term, namely $\sum_{k=j+1}^{n_i+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i]$, we note that $i = p$, which means that $y_0 = y_0^i = y_0^p$, and $j < k$. Hence, by Claim 3.2(b), $Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \leq \frac{1}{2^{l-m}}$, where $k - j = d \times 2^m$ and d is odd. Since $k = j+1, \cdots, n_i+1$, it follows that $k - j = 1, \cdots, n_i - j + 1$, and by Fact 3 with $N - 1 = n_i + 1 - j$ and $a = k - j$,

$$\begin{aligned}\sum_{k=j+1}^{n_i+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \quad &= \quad \sum_{k-j=1}^{n_i-j+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \leq \frac{1}{2^l}\sum_{k-j=1}^{n_i-j+1} 2^m \\ &\leq \frac{1}{2^l}\frac{n_i-j+1}{2}(\log_2(n_i-j+1)+3).\end{aligned}$$

Now, we add the bounds of the last three of the individual upper bounds, and then we add the first upper bound to obtain the total upper bound for forgeries of type (b2).

$$\begin{aligned}&\sum_{k=1}^{j-1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] + Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_j^i] + \sum_{k=j+1}^{n_i+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \leq \\ &\quad \frac{1}{2^l}\frac{j-1}{2}(\log_2(j-1)+3) + \frac{1}{2^l}\frac{n_i-j+1}{2}(\log_2(n_i-j+1)+3).\end{aligned}$$

Since for this type of forgeries $1 \le j \le n_i + 1$, the terms under $\log_2$ are $j-1 \le n_i, n_i - j + 1 \le n_i$. Thus, the sum of the last three terms is bounded as follows:

$$\sum_{k=1}^{j-1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] + Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_j^i] + \sum_{k=j+1}^{n_i-j+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^i] \le$$
$$\frac{1}{2^l}\frac{j-1}{2}(\log_2 n_i + 3) + \frac{1}{2^l}\frac{n_i - j + 1}{2}(\log_2 n_i + 3) = \frac{1}{2^l}\frac{n_i}{2}(\log_2 n_i + 3) \le$$
$$\frac{1}{2^l}\frac{n_i+1}{2}(\log_2 (n_i+1) + 3).$$

Hence, by adding the first of the individual upper bounds to this above sum, we obtain:

$$\begin{aligned}\sum_{p=1}^{q_e}\sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] &\le \frac{1}{2^l}\frac{n_i+1}{2}(\log_2(n_i+1)+3) + \\ &\quad \frac{1}{2^l}\sum_{p=1, p\ne i}^{q_e}\frac{n_p+1}{2}(\log_2(n_p+1)+3) \\ &= \frac{1}{2^l}\sum_{p=1}^{q_e}\frac{n_p+1}{2}(\log_2(n_p+1)+3).\end{aligned}$$

Since $\sum_{p=1}^{q_e}(n_p+1) \le \frac{\mu_e}{l}$, by Fact 4, it follows that

$$Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}] \le$$
$$\sum_{p=1}^{q_e}\sum_{k=1}^{n_p+1} Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] \le \frac{1}{2^l}\frac{\mu_e}{2l}\left(\log_2 \frac{\mu_e}{l} + 3\right).$$

Further, if $m = \max(n_p + 1)$, then $Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}] \le \frac{1}{2^l}\frac{\mu_e}{2l}(\log_2 m + 3)$.

Finally, for any forgery that is not a truncation, $Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}]$ is bounded by the maximum of the bounds for the types (a), (b1) and (b2), namely

$$Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}] \le \frac{1}{2^l}\frac{\mu_e}{2l}\left(\log_2 \frac{\mu_e}{l} + 3\right);$$

or, if $m = \max(n_p + 1)$, then $Pr_{\overline{I} \text{ and } \overline{E}}[z_j \in \{z_k^p, 1 \le p \le q_e, 1 \le k \le n_p + 1\}] \le \frac{1}{2^l}\frac{\mu_e}{2l}(\log_2 m + 3)$. Hence, returning to the probability of event C conditioned by ($\overline{I}$ and $\overline{E}$),

$$Pr_{\overline{I} \text{ and } \overline{E}}[C] = Pr[C \mid \overline{I} \text{ and } \overline{E}] \le \frac{(n+1)q_e}{2^l} + \frac{1}{2^l}\frac{\mu_e}{2l}\left(\log_2 \frac{\mu_e}{l} + 3\right).$$

Also, if the maximum length m of the encrypted messages is known, the last term of the above bound can be replaced with $\frac{1}{2^l}\frac{\mu_e}{2l}(\log_2 m + 3)$. □

Proof of Claim 4

Event $\overline{C}$ is true implies that there is at least one element $z_s \in Z$. Event $\overline{D}$ states that any hidden ciphertext block $z_s \in Z$ collides with another hidden block $z_t \in Z, t \ne s$, or z_s collides with y_0. Hence, $\overline{D} \Rightarrow (z_s = z_t,$ for some $s, t, 1 \le s, t \le n+1, z_s, z_t \in Z, s \ne t$ or $z_s = y_0)$. This implies that

$$Pr[\overline{D} \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}] \le Pr[(z_s = z_t, z_s, z_t \in Z, t \ne s) \text{ or } z_s = y_0 \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}]$$

Union bound leads to:

$$Pr[\overline{D} \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}] \leq Pr[z_s = z_t, z_s, z_t \in Z, t \neq s \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}]$$
$$+ Pr[z_s = y_0 \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}]$$

To compute the upper bound of the first probability of the sum, $Pr[z_s = z_t, z_s, z_t \in Z, t \neq s \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}]$, recall that Z must have at least one element (since $\overline{C}$ is true). If Z has only one element, then this probability is zero. If Z has at least two elements, z_s, z_t, we use the following claim, whose proof can be found at the end of this Appendix:

Claim 4.1
(a) For any $z_s, z_t \in Z, 1 \leq s < t \leq n+1$:

$$Pr_{\overline{C} \text{ and } \overline{E} \text{ and } \overline{I}}[z_s = z_t] \leq \frac{1}{2^{l-m}},$$

where the exponent m is defined by $t - s = d \times 2^m$ and d is odd.
(b) For any $z_s \in Z, 1 \leq s \leq n+1$, and for any y_0:

$$Pr_{\overline{C} \text{ and } \overline{E} \text{ and } \overline{I}}[z_s = y_0] \leq \frac{1}{2^{l-m}},$$

where the exponent m is defined by $s = d \times 2^m$ and d is odd.

Then, by Claim 4.1(a)

$$Pr[z_s = z_t, z_s, z_t in Z, t \neq s \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}] \leq \frac{2^m}{2^l}$$

where $m \leq \log_2(t-s)$ if $t > s$, or $m \leq \log_2(s-t)$ if $t < s$. But, $|t-s| \leq n$; hence $m \leq \log_2 n$, and then $2^m \leq n$. Thus,

$$Pr[z_s = z_t, z_s, z_t \in Z, t \neq s \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}] \leq \frac{n}{2^l}.$$

To compute an upper bound for the second probability of the above sum, namely on $Pr[z_s = y_0 \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}]$, we use Claim 4.1(b) and obtain:

$$Pr[z_s = y_0 \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}] \leq \frac{1}{2^{l-m}},$$

where m is defined by $s = d \times 2^m$ and d is odd. By definition, $m \leq \log_2 s \leq \log_2(n+1)$, and hence $2^m \leq n+1$. Thus,

$$Pr[z_s = y_0 \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}] \leq \frac{n+1}{2^l}.$$

By adding the two upper bounds, it follows that

$$Pr[\overline{D} \mid \overline{C} \text{ and } \overline{E} \text{ and } \overline{I}] \leq \frac{n}{2^l} + \frac{n+1}{2^l} = \frac{2n+1}{2^l}.$$

$\square$

Proof of Fact 1

Let A be an adversary attacking the $XCBC\$-XOR$ mode using q_e+q_v queries, $\mu_e+\mu_v$ total memory for these queries, and time t_e+t_v. The probability of success is related directly to the security of the underlying encryption mode XCBC$ and F. To find an upper bound for this probability, we introduce a distinguisher D for F, which is given two oracles f and f^{-1}, where f is a permutation used by the $XCBC\$-XOR$ mode. D runs A, simulates an oracle for $XCBC\$-XOR$ via queries for its own oracles f and f^{-1}, responds to A's q_e encryption queries, and verifies A's choices of ciphertext forgeries $y'^i = y_0'^i y_1'^i \cdots y_n'^i, y_{n+1}'^i, 1 \le i \le q_v$. D returns the result of each y'^i's decryption to A; i.e., D returns either x'^i or $Null$ to A. D outputs 1 if A's forgery decrypts successfully, and 0, otherwise.

Distinguisher D's advantage, $Adv_D(F,R) \le \epsilon$, is defined as:

$$Adv_D(F,R) = Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[D^f = 1] - Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[D^f = 1].$$

where $f \stackrel{\mathcal{R}}{\leftarrow} F$ denotes the selection of function f from F by the random key K, and $f \stackrel{\mathcal{R}}{\leftarrow} R$ denotes the random selection of f from R.

By the definition of the distinguisher algorithm:

$$Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[D^f = 1] = Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[\mathcal{D}-XCBC\$-XOR(y) \ne Null] = Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[Succ]$$

and

$$Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[D^f = 1] = Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[\mathcal{D}-XCBC\$-XOR(y) \ne Null] = Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[Succ].$$

The above probabilities are over the random choice of r_0, $f \stackrel{\mathcal{R}}{\leftarrow} F$, $f \stackrel{\mathcal{R}}{\leftarrow} R$, and D's guesses. Hence,

$$\begin{aligned} Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[Succ] &= Pr_{f \stackrel{\mathcal{R}}{\leftarrow} F}[Succ] - Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[Succ] + Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[Succ] \\ &= Adv_D(F,R) + Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[Succ] \le \epsilon + Pr_{f \stackrel{\mathcal{R}}{\leftarrow} R}[Succ]. \end{aligned}$$

□

Proof of Fact 2

If $i = d \times 2^m$, then $i \times r_0 = d \times 2^m \times r_0$ has (at least) the first (i.e., least significant) m bits zero. Also, since $i < 2^l$, it follows that $d < 2^{l-m}$. Let $r_{0m} = r_0[1 \cdots l-m]$ be the least significant $l-m$ bits of r_0. (These bits will be shifted in the most significant $l-m$ bit positions of a block by multiplication with 2^m.)

First, we note that

$$i \times r_0 = (dr_{0m})||\underbrace{0 \cdots 0}_{m}$$

where $dr_{0m} = \underbrace{r_{0m} + \cdots + r_{0m}}_{d\ times} \bmod 2^{l-m}$ and $||$ is the concatenation operator. To see this:

$$\begin{aligned} i \times r_0 &= (d \times 2^m) \times r_0 = d \times (r_0 \times 2^m) = \underbrace{(r_0 \times 2^m) + \cdots + (r_0 \times 2^m)}_{d\ times} \\ &= \underbrace{(r_{0m}||\underbrace{0 \cdots 0}_{m}) + \cdots + (r_{0m}||\underbrace{0 \cdots 0}_{m})}_{d\ times} = (\underbrace{r_{0m} + \cdots + r_{0m}}_{d\ times})||\underbrace{0 \cdots 0}_{m} \\ &= (dr_{0m})||\underbrace{0 \cdots 0}_{m} \end{aligned}$$

where $dr_{0m} = \underbrace{r_{0m} + \cdots + r_{0m}}_{d\ times} \mod 2^{l-m}$.

Second, we divide all values of an arbitrary constant a into two complementary classes based on whether the first (i.e., least significant) m bits of a are all zero, compute $Pr[i \times r_0 = a]$ for each class separately, and then take the maximum of the two probabilities as the overall bound.

Let $a[1 \cdots m] = 0$ denote the values of a for which the first m bits are zero, and $a[1 \cdots m] \neq 0$ those for which at least one of the the first m bits is not zero. Since $i \times r_0 = (dr_{0m}) || \underbrace{0 \cdots 0}_{m}$, it follows that, if $a[1 \cdots m] \neq 0$, $Pr[\ i \times r_0 = a\ ] = 0$. However, if $a[1 \cdots m] = 0$, then $[\ i \times r_0 = a\ ] \Leftrightarrow [\ dr_{0m} = b\ ]$, where $b = a[m+1 \cdots l]$ represents bits $m+1, \cdots l$ of a, i.e., the $l-m$ most significant bits of a. Hence, in this case,

$$Pr[\ i \times r_0 = a\ ] = Pr[\ dr_{0m} = b\ ],$$

where $d, r_{0m}, b \in \{0,1\}^{l-m}$. However, d and 2^{l-m} are relatively prime because d is odd. Hence, d has a left inverse,[9] e, and $dr_{0m} = b \Leftrightarrow edr_{0m} = eb \Leftrightarrow r_{0m} = eb \pmod{2^{l-m}}$, which happens with probability $1/2^{l-m}$ because $r_{0m} = r[1 \cdots l-m]$ is random and uniformly distributed in $\{0,1\}^{l-m}$. Thus, if $a[1 \cdots m] = 0$,

$$Pr[i \times r_0 = a] = \frac{1}{2^{l-m}}.$$

Hence, for any value of constant a, $Pr[i \times r_0 = a] \leq \frac{1}{2^{l-m}}$. □

Proof of Fact 3

Since any a can be expressed as $a = d \times 2^m$, where d is odd, there are multiple values of a that have the same exponent m. (For example, for all odd values of a, $m = 0$, and for all even values of a that are not a multiple of 4, $m = 1$.) Hence, when computing the sum $\sum_{a=1}^{N-1} 2^m$, we can group together the terms 2^m that have the same exponent m (i.e., we group the terms 2^m that are equal).

For a given exponent m, we find the number of distinct values of a that have the same exponent m when represented as $d \times 2^m$. To find this number, we note that $1 \leq a \leq N-1$ and, hence, $1 \leq d \leq \lfloor \frac{N-1}{2^m} \rfloor$. Hence, the number of distinct values of a that yield the same exponent m is $\lfloor \frac{1}{2} \left(\lfloor \frac{N-1}{2^m} \rfloor + 1 \right) \rfloor$, since this number is bounded by the number of distinct values of d odd.

From the definition of exponent m, $2^m \leq N-1$ (i.e., $0 \leq m \leq \log_2(N-1)$). Hence,

$$\begin{aligned}\sum_{a=1}^{N-1} 2^m &= \sum_{m=0}^{\lfloor \log_2(N-1) \rfloor} \lfloor \frac{1}{2} \left(\lfloor \frac{N-1}{2^m} \rfloor + 1 \right) \rfloor 2^m \leq \sum_{m=0}^{\lfloor \log_2(N-1) \rfloor} \left(\frac{N-1}{2} + \frac{2^m}{2} \right) \\ &= \frac{N-1}{2}(\lfloor \log_2(N-1) \rfloor + 1) + \frac{2^{\lfloor \log_2(N-1) \rfloor + 1} - 1}{2}\end{aligned}$$

because, for any $M > 0$, $\sum_{m=0}^{M} 2^m = 2^{M+1} - 1$. Hence,

$$\sum_{a=1}^{N-1} 2^m \leq \frac{N-1}{2}(\log_2(N-1) + 1) + (N-1) = \frac{N-1}{2}(\log_2(N-1) + 3).$$

[9] A way to see that d has a left inverse, e, is to label $2^{l-m} = f$, and to note that, if d and f are relatively prime, then, by Euclid's gcd algorithm, there exists e and h such that $ed + hf = 1$; i.e., $ed = 1 - hf$ or $ed = 1 (\text{mod} f)$.

$\square$

Proof of Fact 4

Since, by hypothesis, $\sum_{p=1}^{q_e}(n_p+1) \le \frac{\mu_e}{l}$, the term under the $\log_2$ is $n_p + 1 \le \frac{\mu_e}{l}$. Hence, we obtain:

$$\sum_{p=1}^{q_e}(n_p+1)\log_2(n_p+1) \le \log_2\frac{\mu_e}{l}\sum_{p=1}^{q_e}(n_p+1),$$

and thus,

$$\sum_{p=1}^{q_e}(n_p+1)\log_2(n_p+1) \le \frac{\mu_e}{l}\log_2\frac{\mu_e}{l}.$$

Further, if $m = \max(n_p+1)$, then $\log_2(n_p+1) \le \log_2 m$. Hence,

$$\sum_{p=1}^{q_e}(n_p+1)\log_2(n_p+1) \le \frac{\mu_e}{l}\log_2 m.$$

$\square$

Proof of Claim 3.1

There are three possible complementary cases to consider:
(1) $y_0 = y_0^i$, for some queried message $i, 1 \le i \le q_e$. Then $r_0 = r_0^i$ is random and uniformly distributed, by definition. Furthermore, if $r_0 = r_0^i \ne r_0^p$, then $i \ne p$ and r_0 is also independent of r_0^p, by definition.
(2) $y_0 = z_j^i$, for some queried message $i, 1 \le i \le q_e, 1 \le j \le n_i + 1$; i.e., y_0 collides with some hidden ciphertext block, z_j^i, generated during the encryption of message i. But this is exactly the event prohibited by $\overline{I}$.
(3) $y_0 \ne y_0^i$ and $y_0 \ne z_k^i$, for all queried messages $i, 1 \le i \le q_e, k \ge 1$. Then $r_0 = f^{-1}(y_0) \ne r_0^i, \forall i, 1 \le i \le q_e$ is random, uniformly distributed and independent of anything else because $f^{-1} \overset{R}{\leftarrow} R$ and f^{-1} has never been invoked with argument y_0. Hence, r_0 is random, uniformly distributed and independent of r_0^p. $\square$

Proof of Claim 3.2

The event $z_j = z_k^p$ is equivalent to $y_j - j\times r_0 = y_k^p - k\times r_0^p \Leftrightarrow j\times r_0 = k\times r_0^p - y_k^p + y_j \Leftrightarrow k\times r_0^p = j\times r_0 - y_j + y_k^p$.
(a) If $y_0 \ne y_0^p$, then $r_0 \ne r_0^p$. Since event $\overline{I}$ is true, then r_0 is random, uniformly distributed, and independent of r_0^p, by Claim 3.1 above. Also, event $\overline{I}$ and $\overline{E}$ implies that r_0 is random, uniformly distributed, and independent of r_0^p by the definition of event E. Thus, $j \times r_0$ is independent of $k \times r_0^p - y_k^p + y_j$ and $k \times r_0^p$ is independent of $j \times r_0 - y_j + y_k^p$, since $j, k > 0$, and y_j, y_k^p, j, k are known constants. Furthermore, event $[z_j = z_k^p] \equiv [j \times r_0 = k \times r_0^p - y_k^p + y_j] \equiv [k \times r_0^p = j \times r_0 - y_j + y_k^p]$. Hence,

$$\begin{aligned} Pr_{\overline{I}\text{ and }\overline{E}}[z_j = z_k^p] &= Pr_{\overline{I}\text{ and }\overline{E}}[j \times r_0 = k \times r_0^p - y_k^p + y_j] \\ &= Pr_{\overline{I}\text{ and }\overline{E}}[k \times r_0^p = j \times r_0 - y_j + y_k^p]. \end{aligned}$$

However, $Pr_{\overline{I}\text{ and }\overline{E}}[j \times r_0 = k \times r_0^p - y_k^p + y_j] \le \frac{1}{2^{l-m_1}}$, where $j = d_1 \times 2^{m_1}$ and d_1 is odd, by Fact 2. Also, $Pr_{\overline{I}\text{ and }\overline{E}}[k \times r_0^p = j \times r_0 - y_j + y_k^p] \le \frac{1}{2^{l-m_2}}$, where $k = d_2 \times 2^{m_2}$ and d_2 is odd. Hence,

$$Pr_{\overline{I}\text{ and }\overline{E}}[z_j = z_k^p] \le \min\left(\frac{1}{2^{l-m_1}}, \frac{1}{2^{l-m_2}}\right) = \frac{1}{2^{l-m}},$$

where $m = \min(m_1, m_2)$.

(b) If $y_0 = y_0^p$, then $r_0 = r_0^p$. Hence,

$$z_j = z_k^p \;\Leftrightarrow\; y_j - j \times r_0 = y_k^p - k \times r_0^p \;\Leftrightarrow\; (k-j) \times r_0 = y_k^p - y_j.$$

Thus,

$$Pr_{\overline{I} \text{ and } \overline{E}}[z_j = z_k^p] = Pr_{\overline{I} \text{ and } \overline{E}}[(k-j) \times r_0 = y_k^p - y_j].$$

However, since event $\overline{I}$ is true, it follows that r_0 is random and uniformly distributed, by Claim 3.1 above. Also, event $\overline{I}$ and $\overline{E}$ implies that r_0 is random and uniformly distributed, by the definition of event E. Since $j, k > 0, j \neq k$, and y_j, y_k^p, j, k are known constants, and $k \neq j$, Fact 2 implies that

$$Pr_{\overline{I} \text{ and } \overline{E}}[(k-j) \times r_0 = y_k^p - y_j] \leq \frac{1}{2^{l-m}}$$

where m is defined by $k - j = d \times 2^m, k > j$ or $j - k = d \times 2^m, j > k$, and d is odd. □

Proof of Claim 4.1

(a) One can write the event $z_t = z_s \;\Leftrightarrow\; (t-s) \times r_0 = y_t - y_s$. Hence,

$$Pr_{\overline{C} \text{ and } \overline{E} \text{ and } \overline{I}}[z_s = z_t] = Pr_{\overline{C} \text{ and } \overline{E} \text{ and } \overline{I}}[(t-s) \times r_0 = y_t - y_s].$$

Since event $\overline{I}$ is true, r_0 is random and uniformly distributed, by Claim 3.1. Furthermore, by the definition of events $\overline{E}$ and $\overline{C}$, event $\overline{C}$ and $\overline{I}$ and $\overline{E}$ implies that r_0 is random and uniformly distributed. Using the definition of m and the facts that (1) r_0 is random and uniformly distributed, (2) y_t, y_s are constants, and (3) $1 \leq t - s \leq 2^l - 1$, we obtain (by Fact 2) that

$$Pr_{\overline{C} \text{ and } \overline{E} \text{ and } \overline{I}}[(t-s) \times r_0 = y_t - y_s] \leq \frac{1}{2^{l-m}}$$

where m is defined by $t - s = d \times 2^m$ and d is odd. Hence,

$$Pr_{\overline{C} \text{ and } \overline{E} \text{ and } \overline{I}}[z_s = z_t] \leq \frac{1}{2^{l-m}}.$$

(b) The proof of this part is similar to that of part (a) and is included here for completeness.

Note that, since $z_s = y_s - s \times r_0$, event $z_s = y_0 \;\Leftrightarrow\; s \times r_0 = y_s - y_0$, where y_s and y_0 are constants. However, since event $\overline{I}$ is true, r_0 is random and uniformly distributed, by Claim 3.1. Furthermore, event $\overline{C}$ and $\overline{I}$ and $\overline{E}$ implies that r_0 is random and uniformly distributed. Hence, by Fact 2,

$$Pr_{\overline{C} \text{ and } \overline{E} \text{ and } \overline{I}}[z_s = y_0] = Pr_{\overline{C} \text{ and } \overline{E} \text{ and } \overline{I}}[s \times r_0 = y_s - y_0] \leq \frac{1}{2^{l-m}}$$

where m is defined by $s = d \times 2^m$ and d is odd. □