Padding Oracle Attacks on CBC Mode Encryption with Secret and Random IVs

Kenny Paterson
Information Security Group
Royal Holloway, University of London
kenny.paterson@rhul.ac.uk

Joint work with Arnold Yau and Chris Mitchell

Overview

- Introduction
  - Review of CBC mode
  - Padding oracle attacks
- ISO standards for CBC mode
  - Padding oracle attacks in the public IV setting
  - Padding oracle attacks for secret and random IVs
- Security of OZ-PAD
- Conclusions

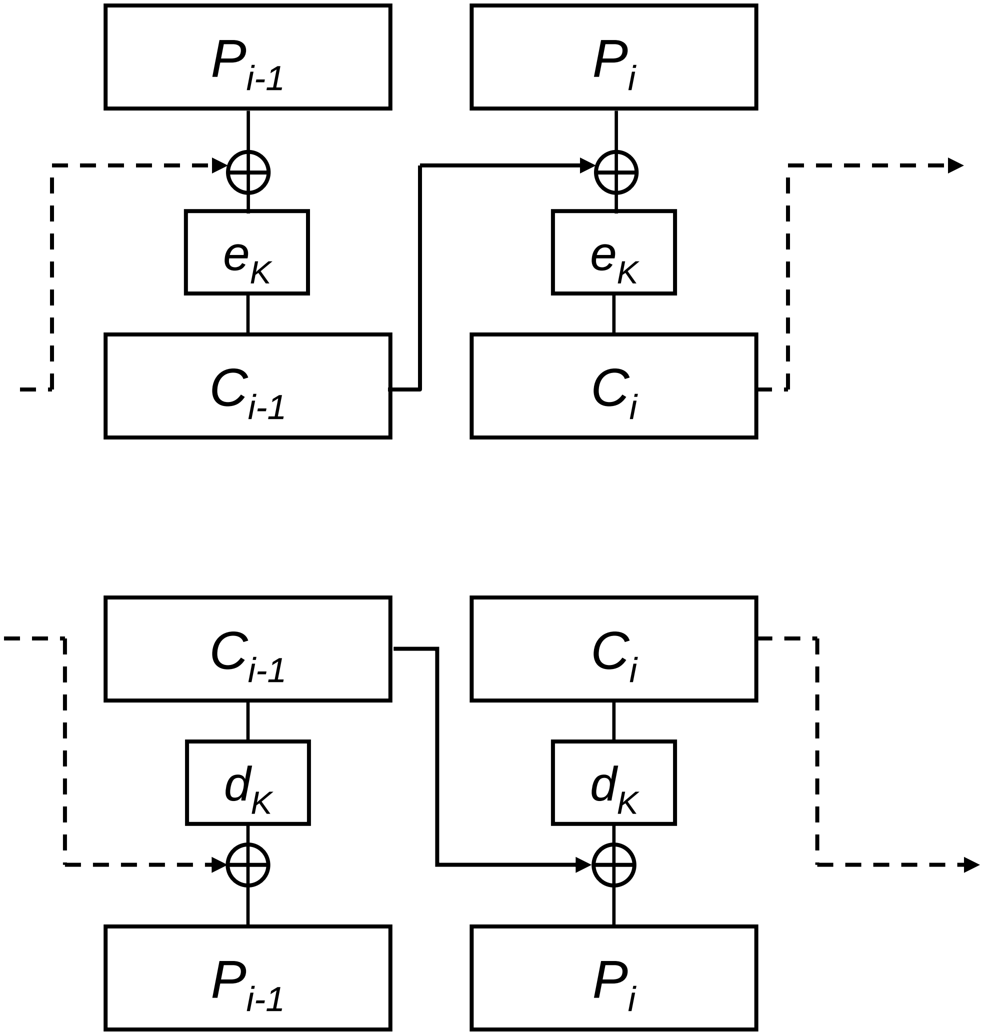
CBC Mode

- CBC mode is a mode of operation for a block cipher.
- Allows encryption of arbitrary length data.
- Data D of length L_D.
- Padded to P blocks $P_1, P_2, \ldots, P_q$.
- Block size n, key K, IV (= C_0).
- Encryption and decryption are defined by

$$C_i = e_K(P_i \oplus C_{i-1})$$

$$P_i = d_K(C_i) \oplus C_{i-1}$$

CBC Mode Encryption and Decryption

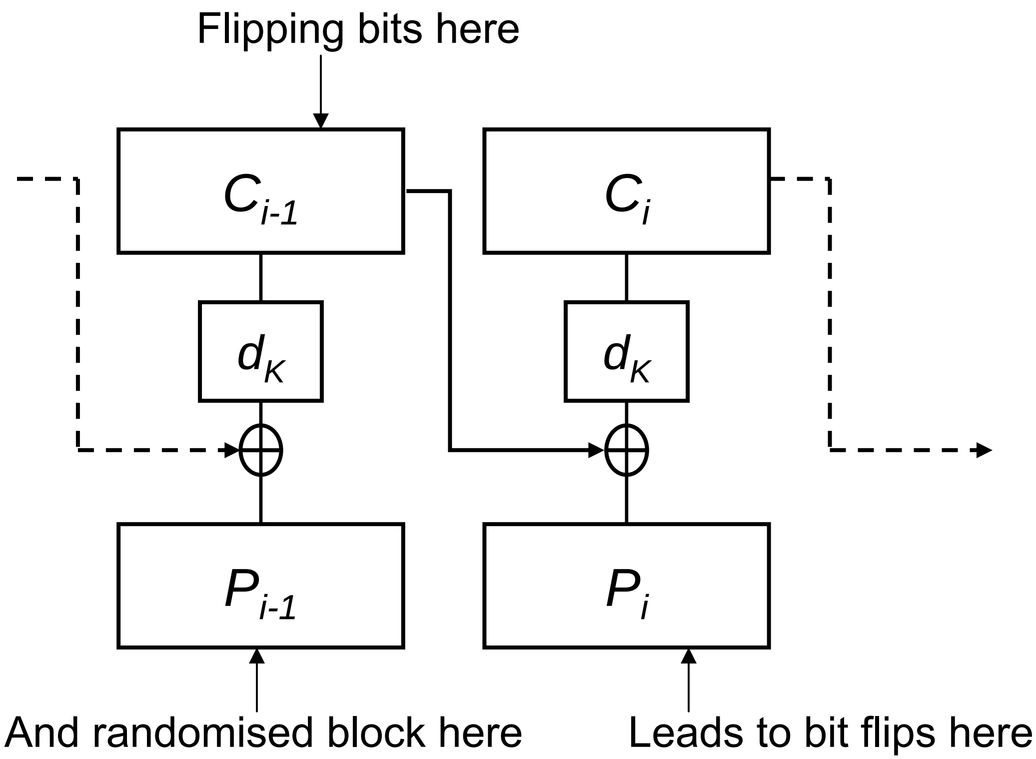


Typical block size *n*:
64 bits (DES, triple DES) or 128 bits (AES).

Typical key size:
56 bits (DES), 168 bits (triple DES), 128, 192 or 256 bits (AES).

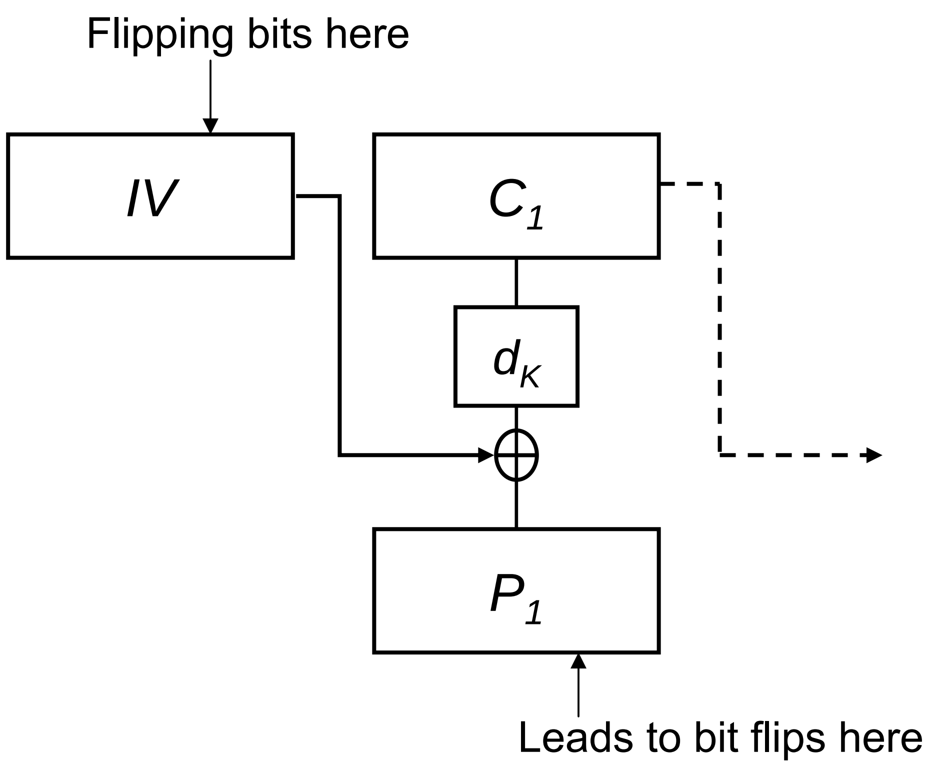
Bit Flipping in CBC Mode

- Flipping bits in ciphertext block C_{i-1} leads to controlled changes in plaintext block P_i.
- Block P_{i-1} is randomised.



Bit Flipping in CBC Mode

- And flipping bits in ciphertext block $C_0 = IV$ leads to controlled changes in plaintext block P_1.



Padding in CBC Mode

- How should padding be added in CBC Mode?
- Numerous possibilities including:
  - Append unique removable pattern (“10…0” or “012…b” or “bb….b”)
  - Append or prepend length information in field of fixed size, pad remaining bits in fixed way (e.g. 0’s).
- Padding can also be used to enhance security
  - Disguise the length of plaintexts
  - Prevent traffic analysis, or guessing based on plaintext length.
  - “*Buy*” versus “*Sell*”.
  - Allowed in IPSec, for example.
- Can padding have a negative impact on security?

Padding Oracle Attacks

- First proposed by Vaudenay (Eurocrypt 2002)
- Assume that a *padding oracle* is available to the adversary.
  - Adversary submits CBC mode ciphertext to oracle.
  - Oracle decrypts under fixed key K and checks correctness of padding with respect to particular padding method in use.
  - Oracle outputs VALID or INVALID according to correctness of padding.
- Vaudenay showed that padding oracles and bit flipping can be used to build decryption oracle for CBC mode.
  - For a variety of padding schemes, including those used in SSL/TLS and IPSec.

Padding Oracle Attacks

- Attack only possible if padding oracle exists in practice.
- Existence of oracle depends on cryptographic implementation.
- Typically, incorrect padding leads to delay in processing or possibly error message.
- Practical implementation of attack on OpenSSL by Canvel, Hiltgen, Vaudenay, Vuagnoux (Crypto 2003)
  - "Dirty" oracle based on timing channel.
  - Attack complicated by SSL session abort in event of padding errror and encrypted error messages.
  - Attack successful in recovering e-mail passwords for IMAP account supposedly protected by SSL.

ISO CBC Mode Standard

- ISO/IEC 10116 standardises modes of operation for block ciphers, including CBC mode.
- Second edition of ISO/IEC 10116 makes no mention of padding methods.
- Third edition now under development.
  - Due for completion in 2005 (?)
- Second Committee Draft (2002) of third edition included padding methods.
  - Padding methods taken from:
    - ISO/IEC 9797-1 (MACs)
    - ISO/IEC 10118-1 (Hash functions)

ISO CBC Mode Standard

- Some padding methods in ISO/IEC 9797-1 and ISO/IEC 10118-1 are vulnerable to padding oracle attacks.
  - Standards include methods with many-to-one padding – we ignore these!
  - Standards include OZ-pad: “10…0”
    - This method appears to be invulnerable to padding oracle attacks (see later).
  - Remaining methods are vulnerable to attack.
    - “Padding oracle attacks on the ISO CBC mode encryption standard”, Paterson and Yau, CT-RSA 2004.
    - Our attacks assume IVs form part of ciphertexts – “the public IV setting”.
    - Bit flipping and a variety of other tricks.

ISO CBC Mode Standard – FCD

- Final Committee Draft (FCD) (2004) of third edition:
  - Removes specification of concrete padding methods.
    - As a consequence of our CT-RSA 2004 paper
  - Makes recommendation that secret and random IVs be used.
    - Use of random IVs needed for security proof for CBC mode
    - Secret IVs recommended “to prevent information leakage”.
  - Earlier attacks from CT-RSA 2004 mostly obviated by following these recommendations.

ISO CBC Mode Standard – FCD

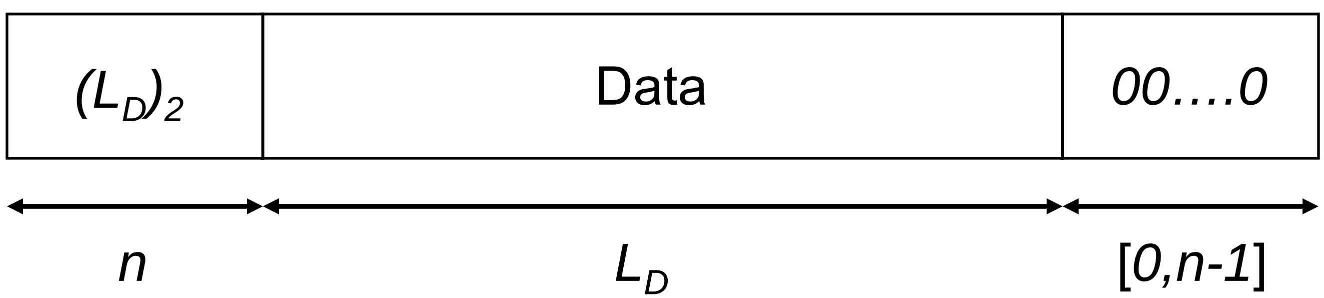
- FCD no longer specifies concrete padding methods.
- So what should an implementer do?
  - Might borrow from existing standards.
  - As did the editor of ISO/IEC 10116 third edition.
- We now focus on attacking padding methods from ISO/IEC 9797-1 and ISO/IEC 10118-1 in the secret and random IV setting.
- Main finding: ISO padding methods are still weak in presence of padding oracle.

Two Models for Secret IVs

- How to ensure both parties share the same IV if IVs are secret and random?
- How to model this in padding oracle attacks?
- Model 1
  - IV-determining information is sent alongside the ciphertext.
    - ECB encryption or decryption of some additional block.
    - Or selection from a pre-shared list of values.
  - Adversary can force re-use of a given (unknown) IV by the padding oracle.
- Model 2
  - No information about IVs sent at all.
  - e.g. synchronised PRNG.
  - Harder attack model for adversary: cannot influence selection of IV used by padding oracle.

Attacking ISO/IEC 9797-1 Padding

- Method 3 of ISO/IEC 9797-1
  - Left-pad data with a block containing data length in binary, right-pad with as few ‘0’s as necessary to complete a block.



ISO/IEC 9797-1 Attack Overview

Information used in attack:

- q-block target ciphertext

  $$C = C_1 \,||\, C_2 \,||\, \ldots \,||\, C_q$$

- Set of auxiliary ciphertexts:

  $$C^1, C^2, \ldots, C^m$$

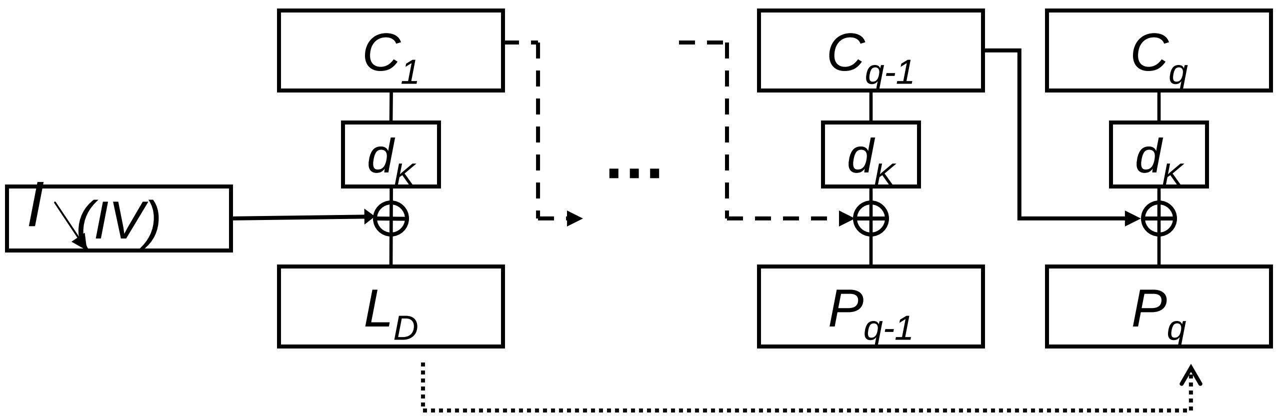
- Along with IV determining info (so in model 1):

  $$I^1, I^2, \ldots, I^m$$

- Phase 1 of attack:
  - determines length of plaintexts corresponding to auxiliary ciphertexts.
- Phase 2 of attack:
  - decrypt any block C_k from target C in segments using length information from Phase 1.

ISO/IEC 9797-1 Attack - Phase 1

Finding L_D:



- Flip bit in C_{q-1} to flip corresponding bit in P_q
- Submit to padding oracle.
- INVALID means padding "0" flipped to "1".
  - padding boundary to left of flip position.
- VALID means data bit flipped.
  - Padding boundary to right of flip position.
- Results in binary search algorithm requiring $\log_2 n$ oracle queries to determine L_D .

ISO/IEC 9797-1 Attack - Phase 1

- Apply this attack to auxiliary ciphertexts

  $$C^1, C^2, \ldots , C^m$$

  to find their lengths

  $$L_1, L_2 , \ldots , L_m$$

  using $m \log_2 n$ oracle queries.
- Assume lengths modulo block length n are

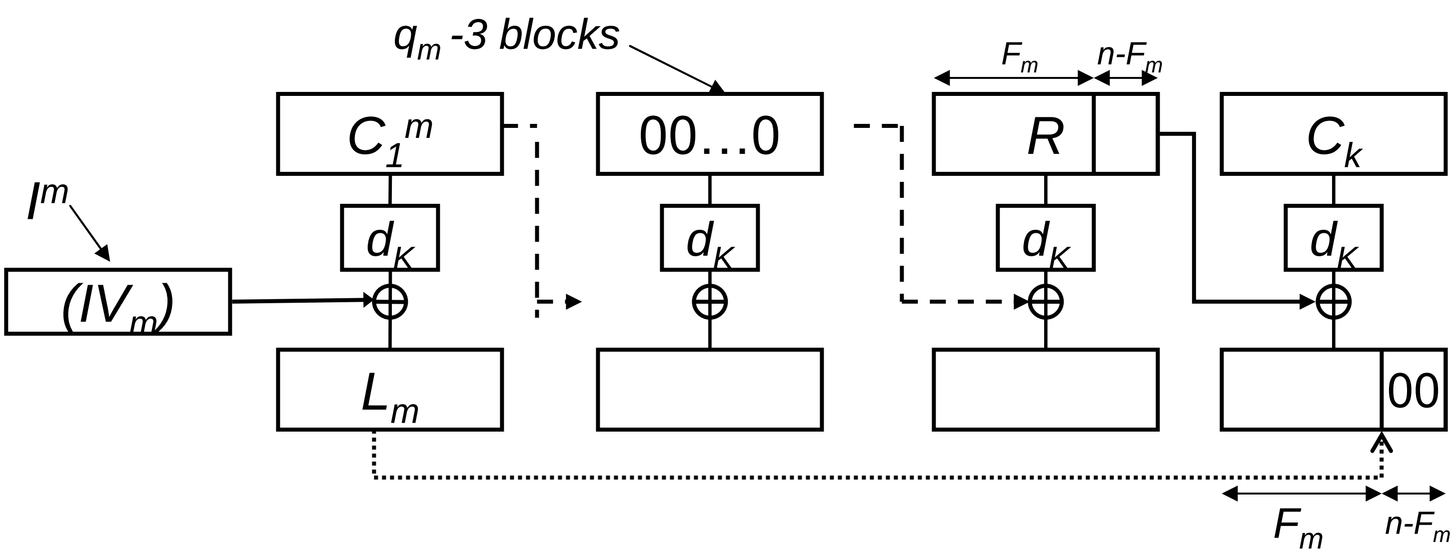
  $$F_1, F_2 , \ldots , F_m$$

  with

  $$1 \leq F_1 < F_2 < \ldots < F_m \leq n\text{-}1.$$

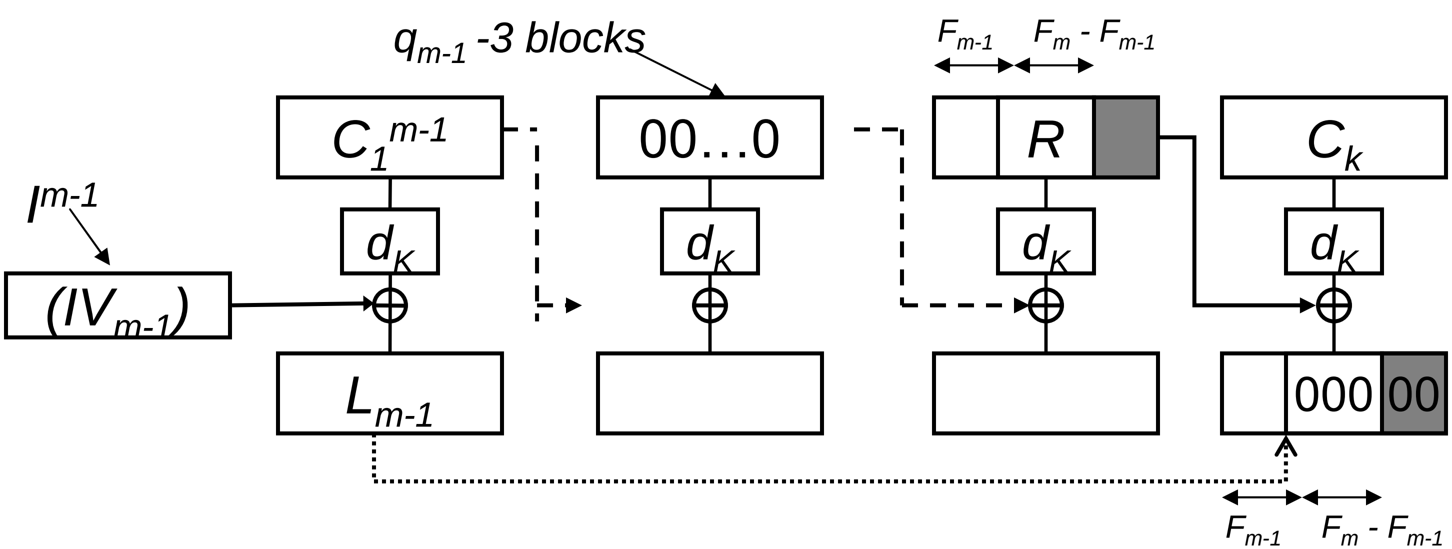
ISO/IEC 9797-1 Attack - Phase 2

- Now attempt to decrypt ciphertext block C_k from target ciphertext.
- Try submitting ciphertexts with all values of R in rightmost n - F_m positions.
- Will receive exactly one VALID response
  - Success implies bits are all ‘0’s in rightmost n - F_m positions



ISO/IEC 9797-1 Attack - Phase 2

- Now fix *R* at these positions to be the successful value.
- And continue attack on positions F_{m-1} to F_m-1 using auxiliary ciphertext C^{m-1}.
- Explore all possible settings of R in these positions.
- Unique valid response implies bits are now all '0's in rightmost $n - F_{m-1}$ positions.
- Repeat with C^{m-2}, C^{m-3}, …



ISO/IEC 9797-1 Attack - Phase 2

- After final iteration of attack:
  - Rightmost n-F_1 bits of final plaintext block are equal to 00…0
  - Hence rightmost n-F_1 bits of P_k are equal to final value of $R \oplus C_{k-1}$
- Average number of oracle queries for Phase 2:

$$\sum_{j=1}^{m} 2^{F_{j+1}-F_j-1}$$

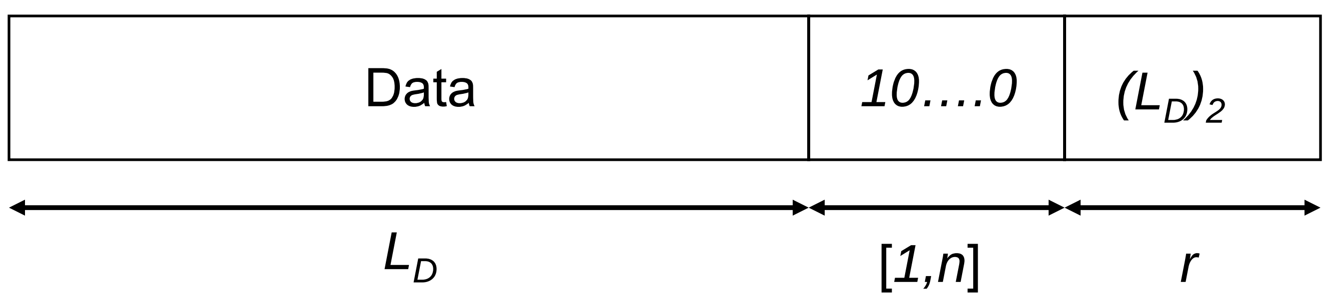
  - Depends on spread of auxiliary ciphertext lengths
    - Byte oriented data, n=64, lengths mod n = 8,16,..,56:
      - about 900 oracle queries to extract 56 out of 64 bits of each plaintext block.

ISO/IEC 9797-1 Attack Summary

- Limitations:
  - Attack does not extract leftmost $F_1 \geq 1$ bits of plaintext of each block.
    - Still an open problem to extract these.
  - Auxiliary ciphertexts have to be at least 3 blocks in length.
  - Auxiliary ciphertexts need to be collected and need to have a reasonable spread of lengths.
    - Auxiliary ciphertexts themselves can of course be decrypted.
- Despite these limitations:
  - Secret and random IV recommendations in ISO/IEC 10116 FCD do not enhance security greatly against padding oracle attacks for this padding method.

Attacking ISO/IEC 10118-1 Padding

- Method 3 of ISO/IEC 10118-1
  - Choose parameter $r \leq n$.
  - Encode L_D in r bits (base 2 assumed).
  - Right-pad a single ‘1’ bit, followed by as few ‘0’s as possible to push the encoded L_D to the end of a block.

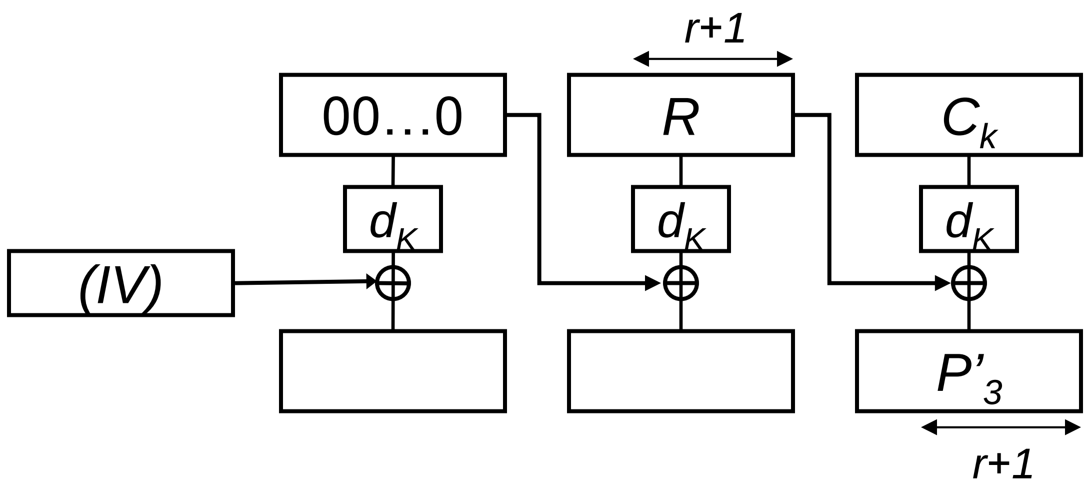


ISO/IEC 10118-1 Attack Overview

- Attacks in (tougher) Model 2
  - IV completely hidden and non-selectable.
  - Adaptations of attacks in CT-RSA 2004 paper.
- First attack: targets arbitrary ciphertext block C_k
  - Construct a valid 3 or 4 block ciphertext having C_k as final block.
- Second attack: efficiently decrypts last block of any ciphertext.
  - Firstly determines L_D efficiently.
  - Secondly decrypts remaining bits in last block efficiently.
  - Similar to L_D-finding attack on ISO/IEC 9797-1.

ISO/IEC 10118-1 First Attack

- Assume $r < n$ for simplicity.
- We construct special three-block ciphertexts and submit them to padding oracle.
- Go through all settings of rightmost $r+1$ bits of R.
- At least one setting will produce matching padding and length fields.
- Padding oracle returns VALID response for this setting.



ISO/IEC 10118-1 First Attack

- Average case complexity of first attack:
  - $r < n$: 2^{r-1} oracle queries.
  - $r = n$: 2^r oracle queries.
- Second attack determines plaintext in last block efficiently.
  - Binary search to discover L_D.
  - Followed by extraction of any data bits in last block.
    - One oracle query per data bit.
  - Apply to 3 block ciphertext constructed in first attack.
    - In final step, modify plaintext with mask $R \oplus C_{k-1}$ to recover original plaintext matching target block C_k.
    - Needs knowledge of C_{k-1} so cannot be applied to block C_1.

ISO/IEC 10118-1 Attack Summary

- Attack can recover all *n* bits of any target block (except for block C_1) many orders faster than exhaustive key search provided *r* is not too large.
- Once again, secret and random IV recommendations in ISO/IEC 10116 FCD do not hinder attack significantly.

Recommendation: OZ-PAD

- One useable method survives from the ISO standards: OZ-PAD:
  - Pad data with a single “1” and as many “0”s are necessary to fill a complete block.
  - May add an entire block in forming CBC plaintext.
- OZ-PAD appears to resist padding oracle attacks against CBC mode.
  - Only get INVALID response if last plaintext block is all zeros.
  - So padding oracle returns VALID with probability $1-2^{-n}$.
  - Then hard for attacker to manipulate last-but-one ciphertext block to get useful information from oracle.
- Our recommendation now adopted in ISO/IEC 10116 Final Distribution (FDIS).

Conclusions (1)

- Padding oracle attacks can be realised in practice.
  - Work of Canvel *et al.* from Crypto 2003.
- Secret and random IVs do not in general prevent padding oracle attacks.
  - They may enhance security in other ways.
    - Use of random IVs supported by security proof.
- Not specifying any padding methods in a standard is a bad idea.
  - Implementer may choose unsafe method and may inadvertently introduce padding oracle in implementation.

Conclusions (2)

- Padding oracle attacks are easily prevented by proper use of strong integrity checks.
  - Use a MAC algorithm, ensure uniform reporting of pad failures and MAC failures if MAC applied before pad and encrypt.
  - Or use an authenticated encryption algorithm.
- Some applications are severely constrained in memory or processing power.
  - Integrity checks may then cost too much.
  - Careful choice of padding method then needed.
- Full paper to appear in Proceedings FSE 2005.