EFAIL

BREAKING S/MIME AND OPENPGP EMAIL ENCRYPTION USING EXFILTRATION CHANNELS

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

Damian Poddebniak[1], Christian Dresen[1], Jens Müller[2], Fabian Ising[1], Sebastian Schinzel[1], Simon Friedberger[3], Juraj Somorovsky[2], Jörg Schwenk[2]

[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)

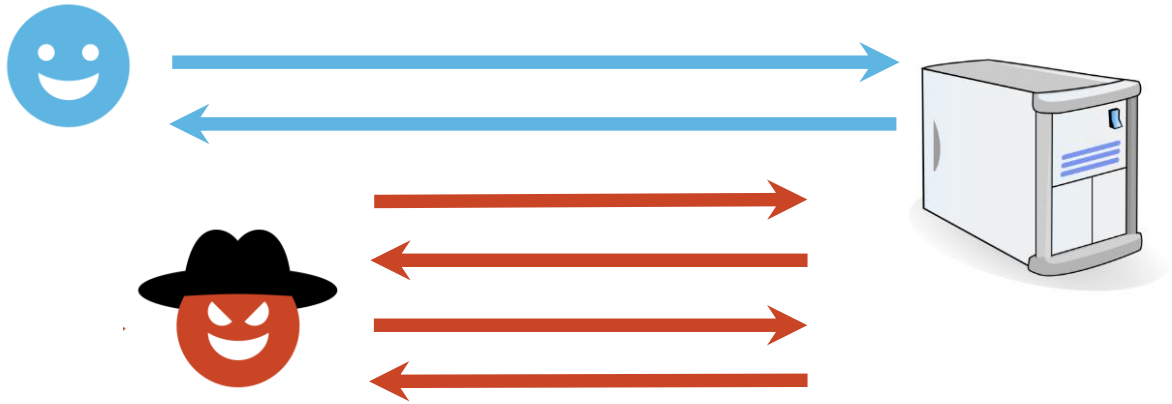
- Favored by privacy advocates
- Web-of-trust (no authorities)

S/MIME (RFC 5751)

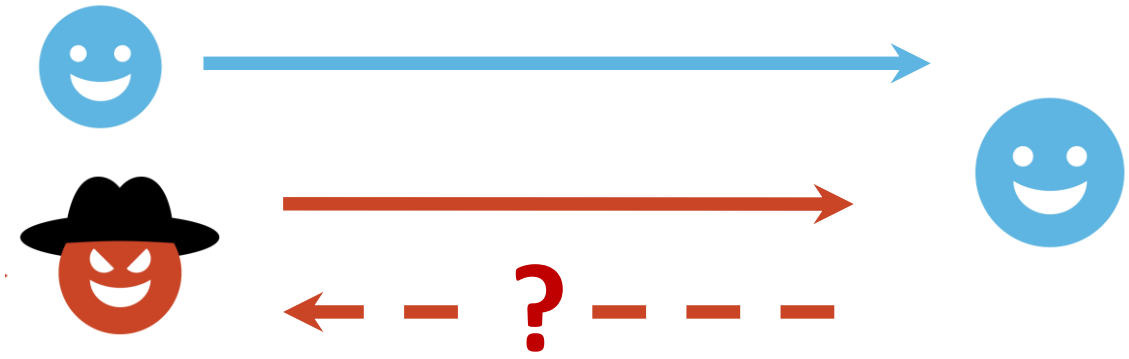
- Favored by organizations
- Multi root trust hierarchies

Security of email encryption

Request/response protocols



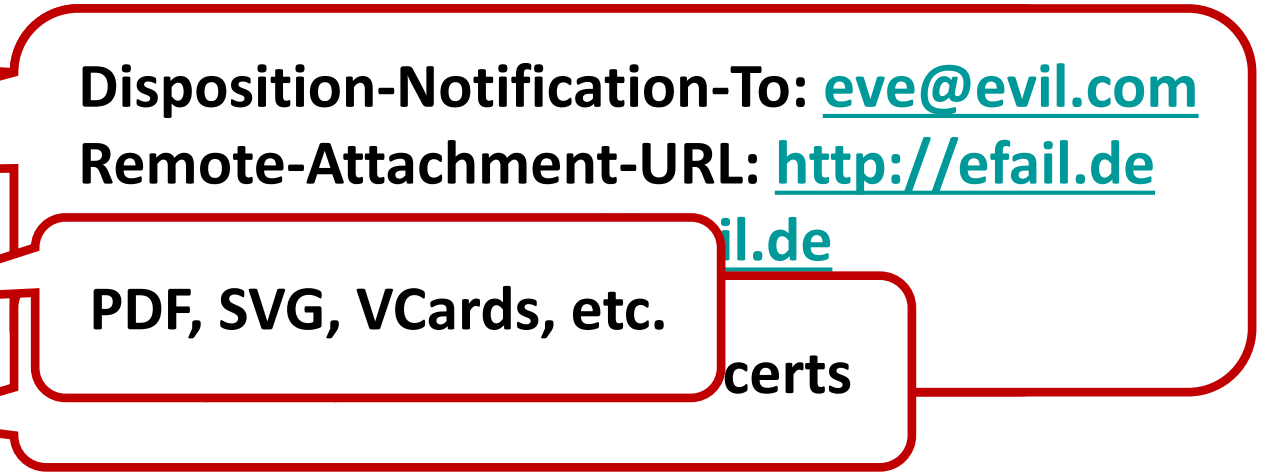
Email is non-interactive



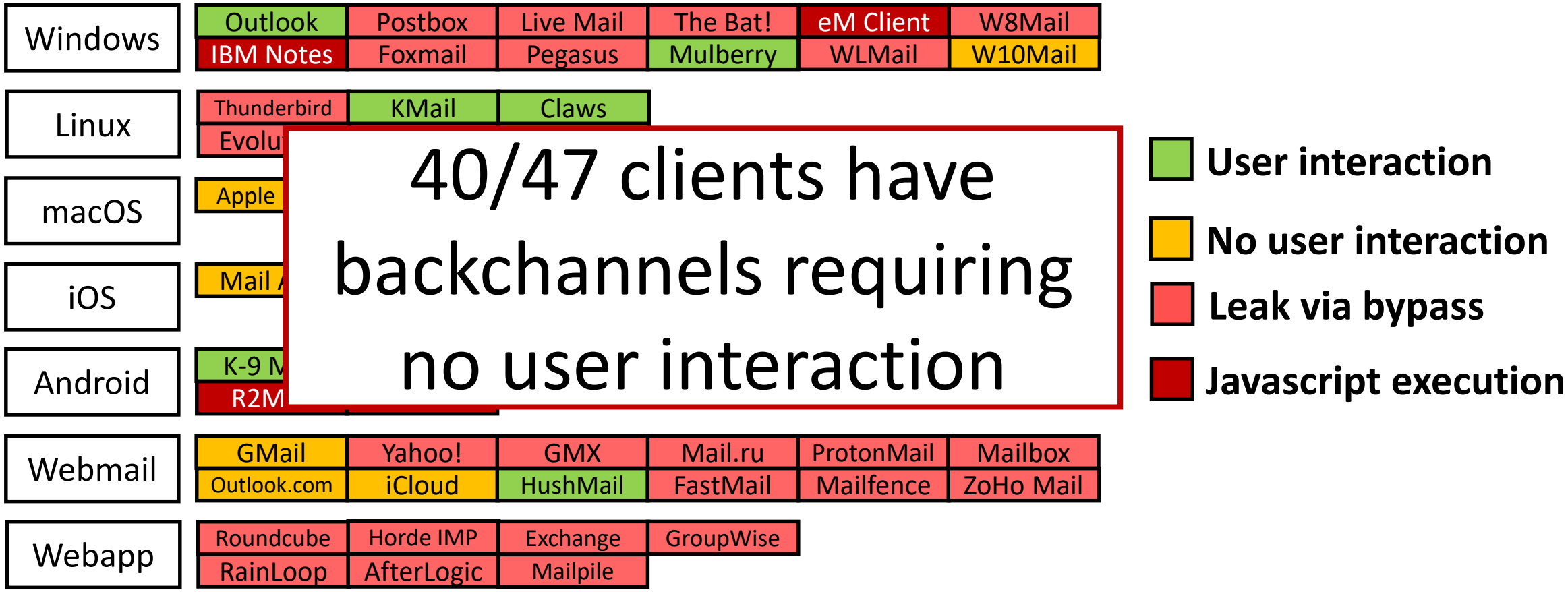
Backchannel techniques

Forcing an email client to send responses via *backchannels*

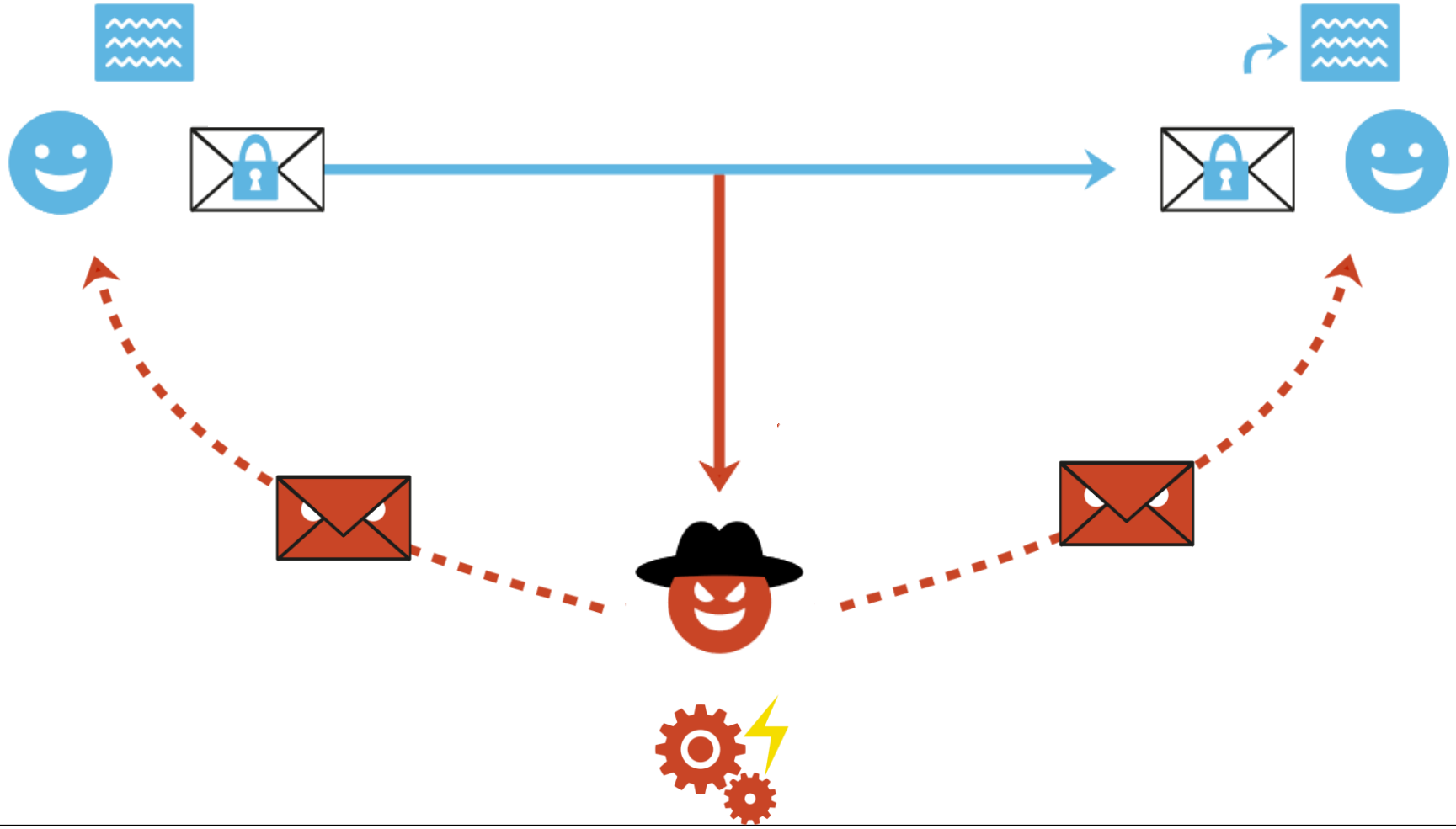
- **HTML/CSS**
- **Email header**
- **Attachment preview**
- **Certificate verification**



Evaluation of backchannels in email clients

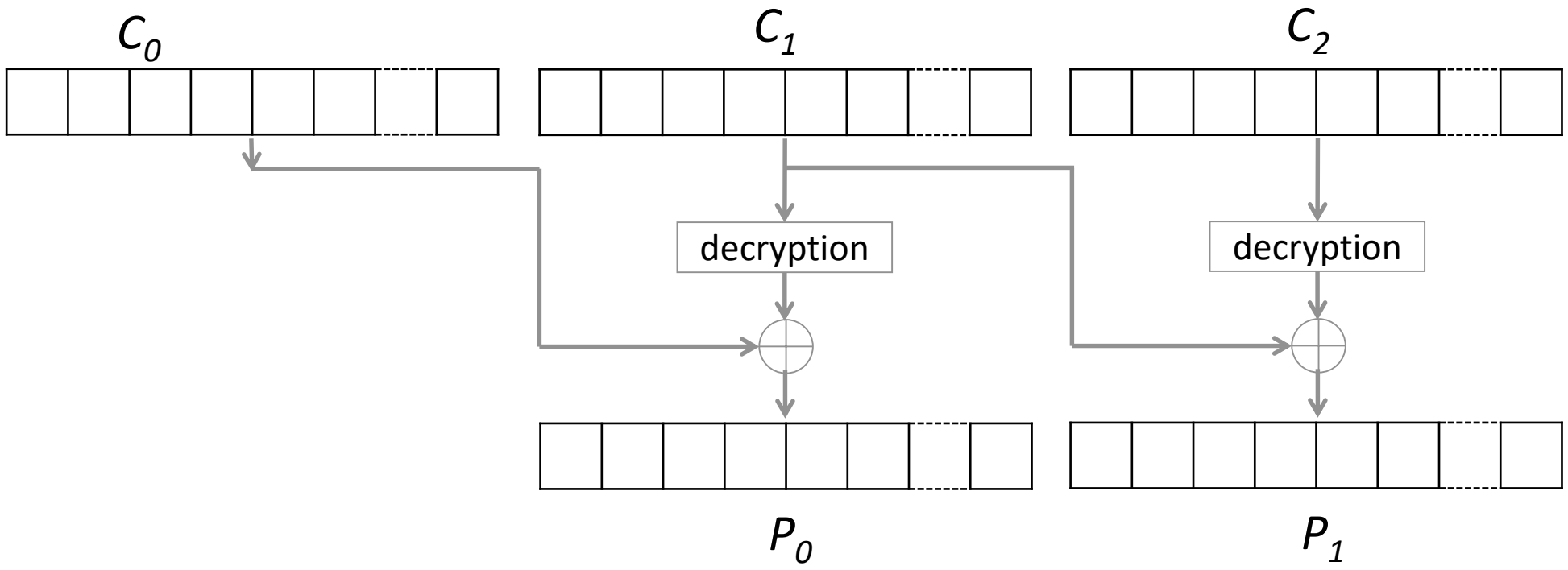


Attacker model

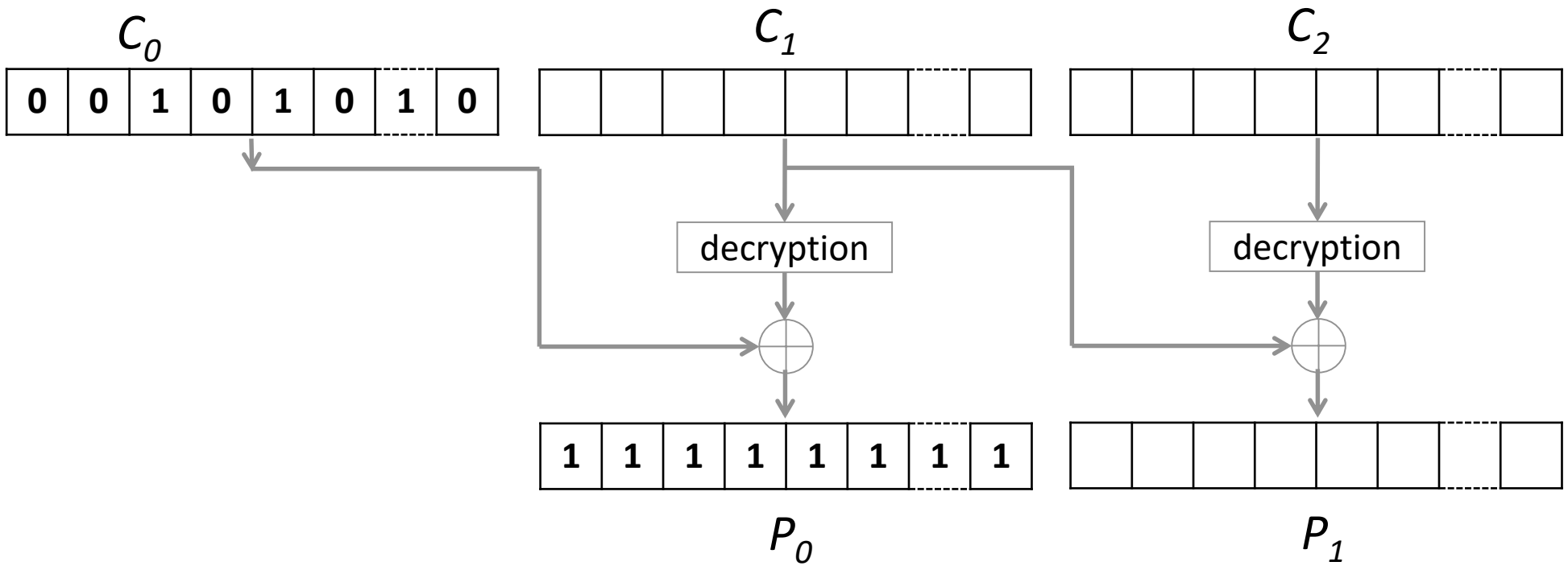


S/MIME

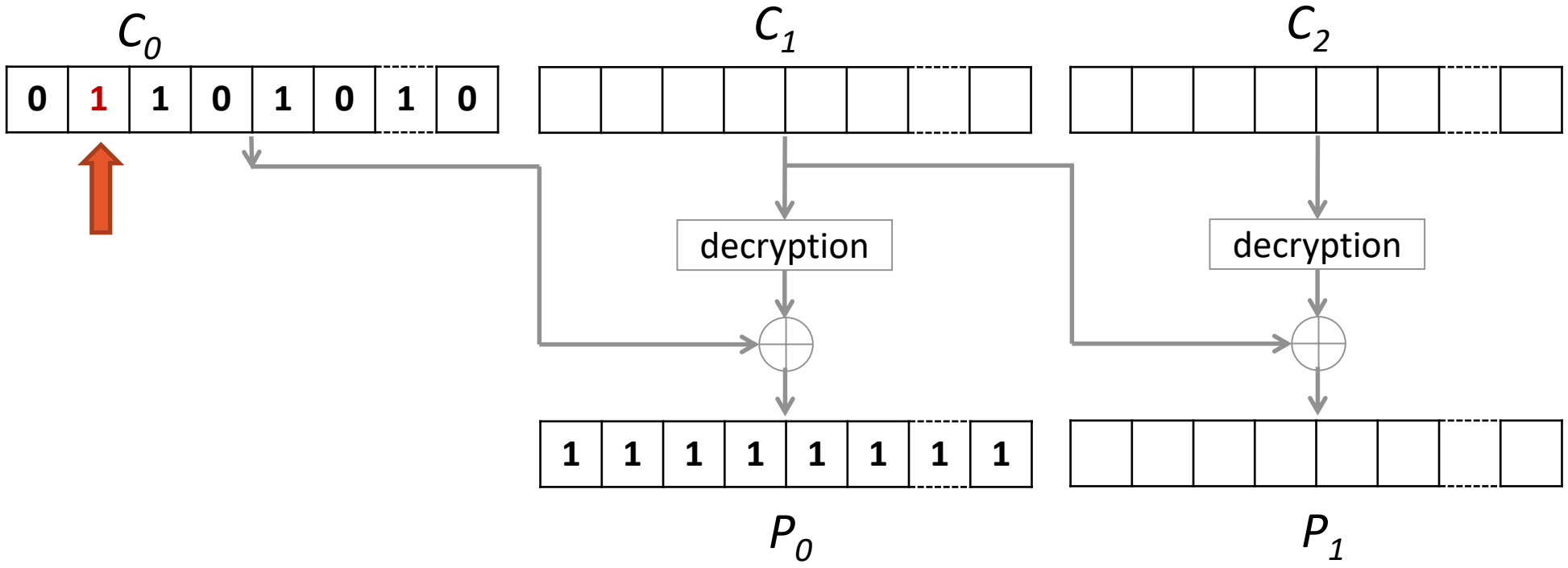
Malleability of CBC



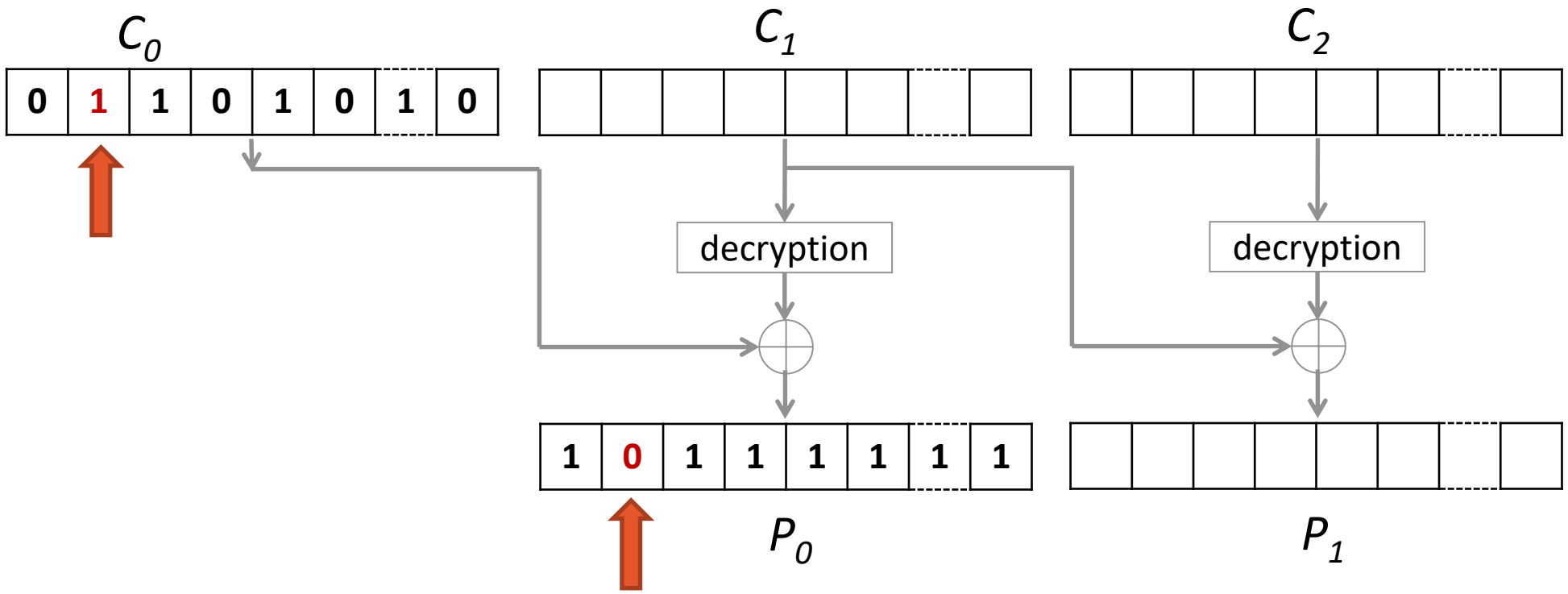
Malleability of CBC



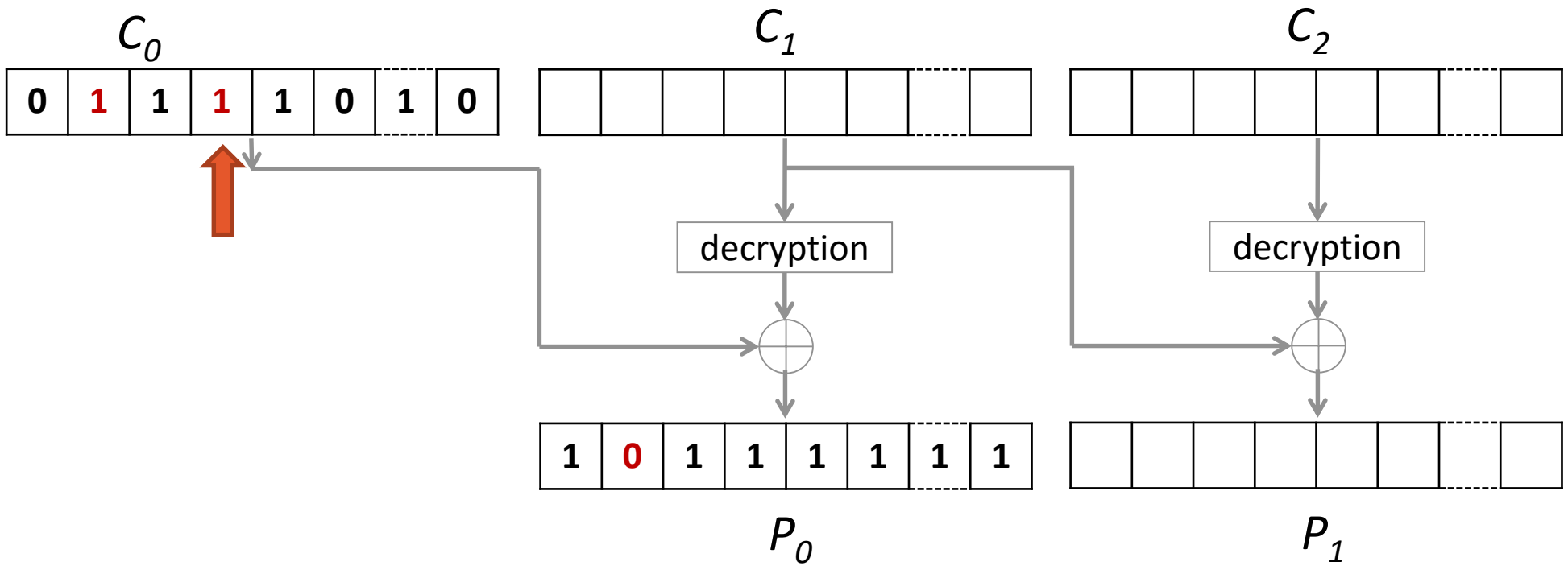
Malleability of CBC



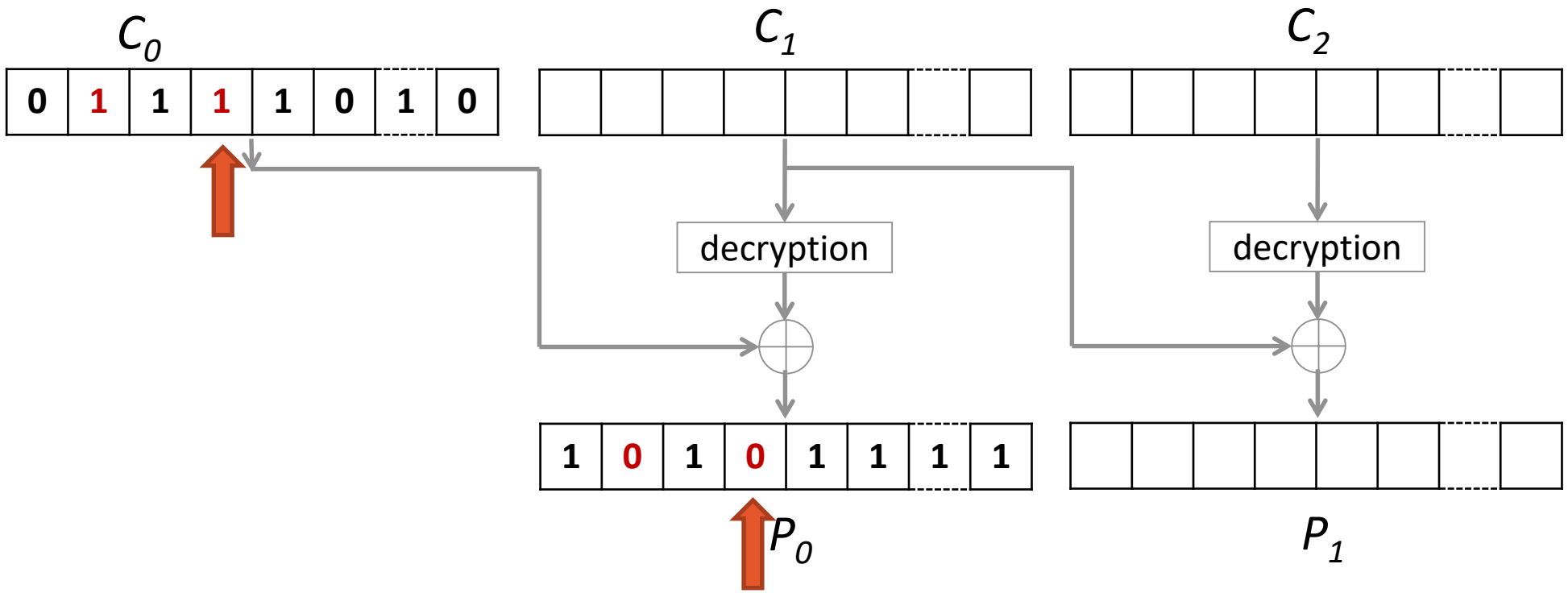
Malleability of CBC



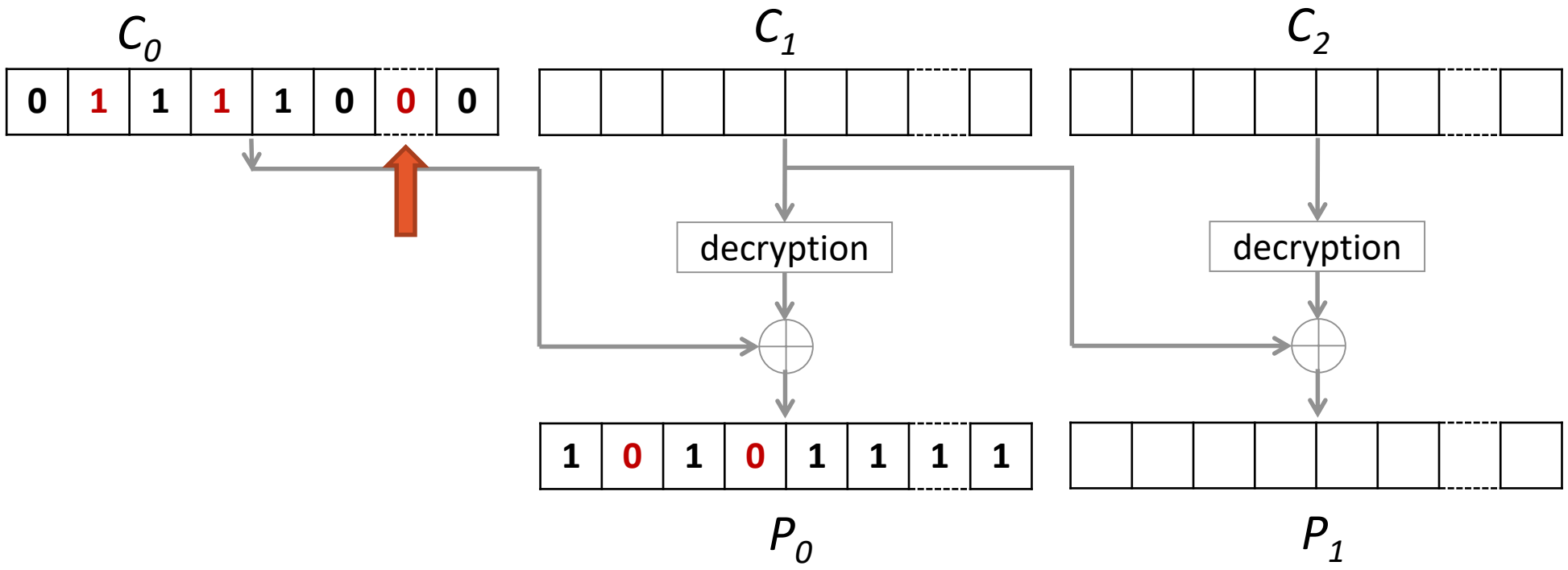
Malleability of CBC



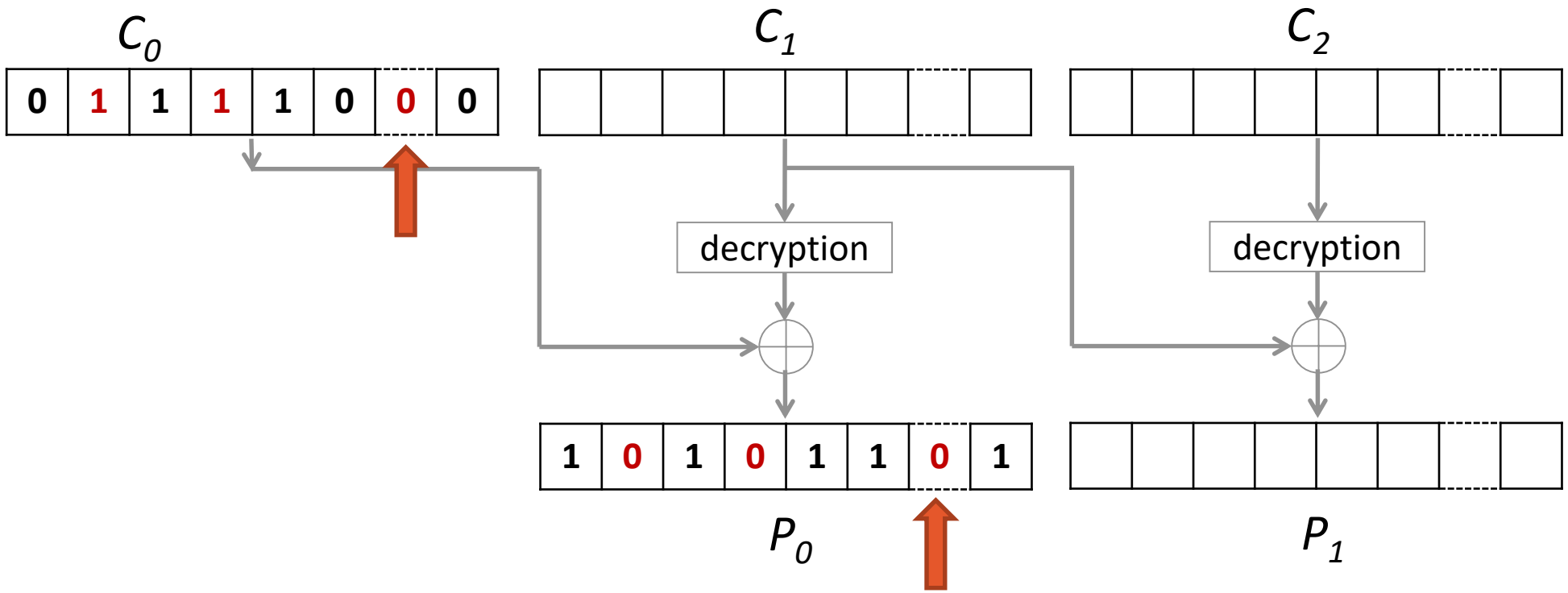
Malleability of CBC



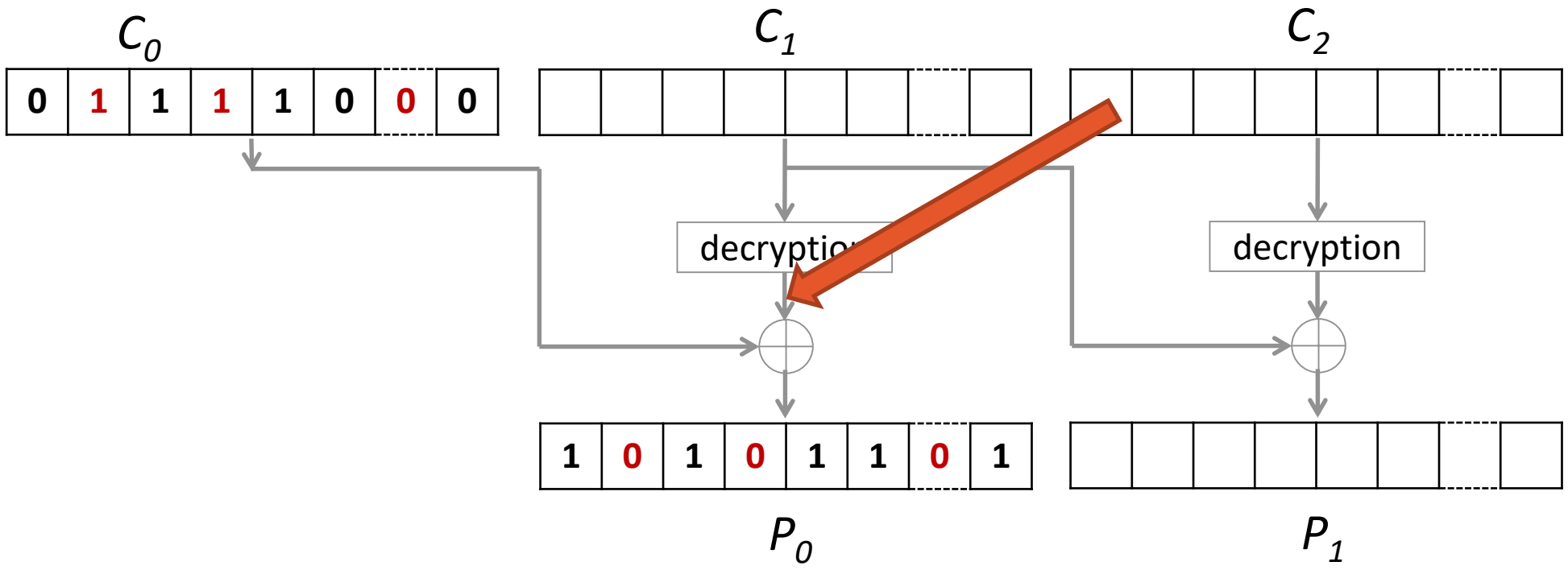
Malleability of CBC



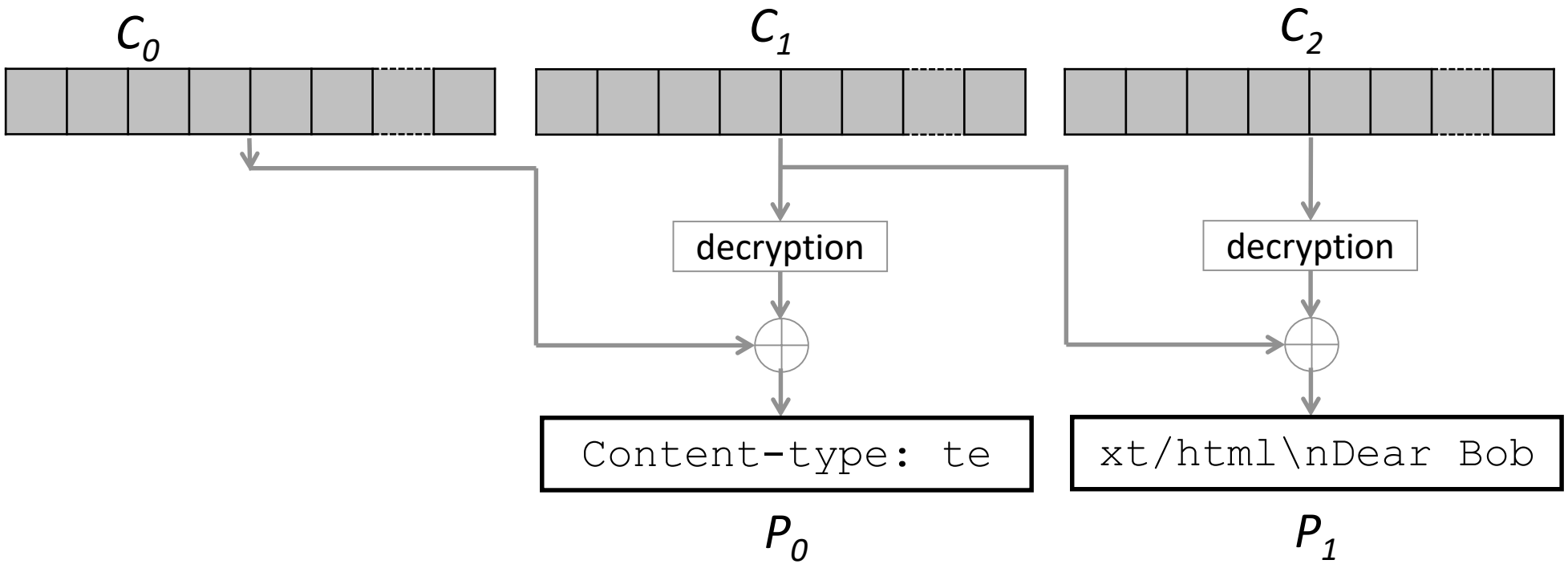
Malleability of CBC



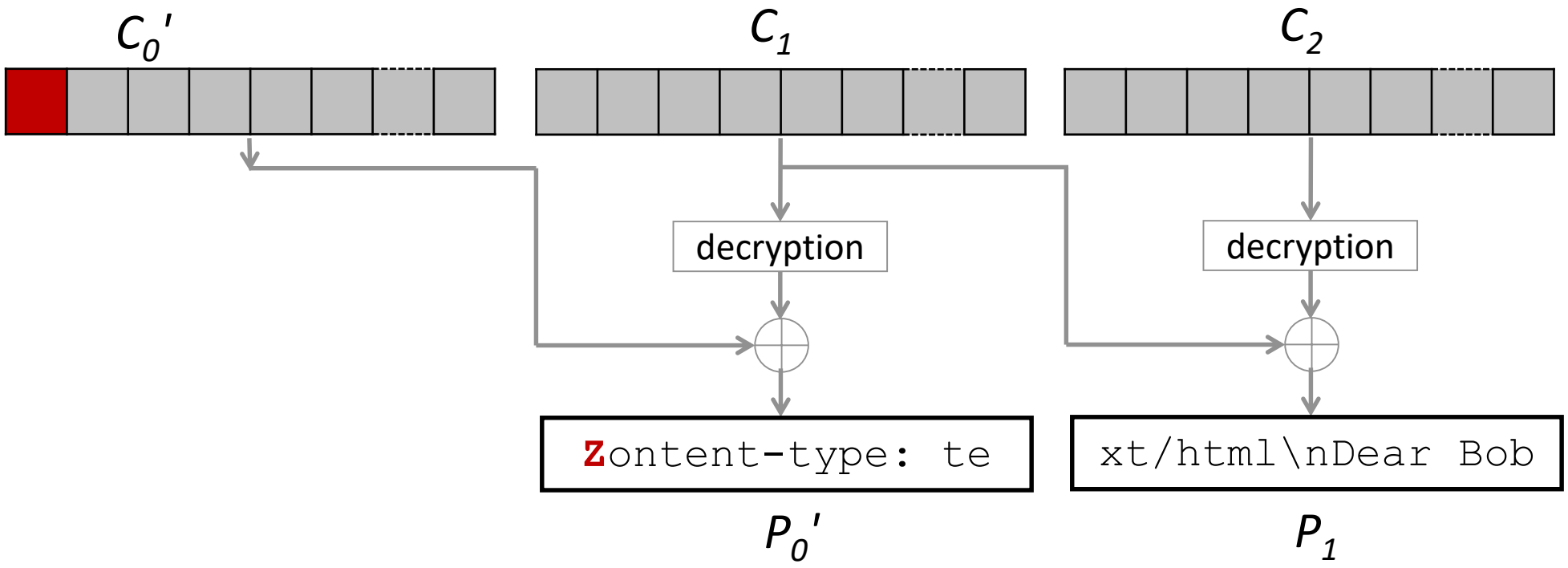
Malleability of CBC



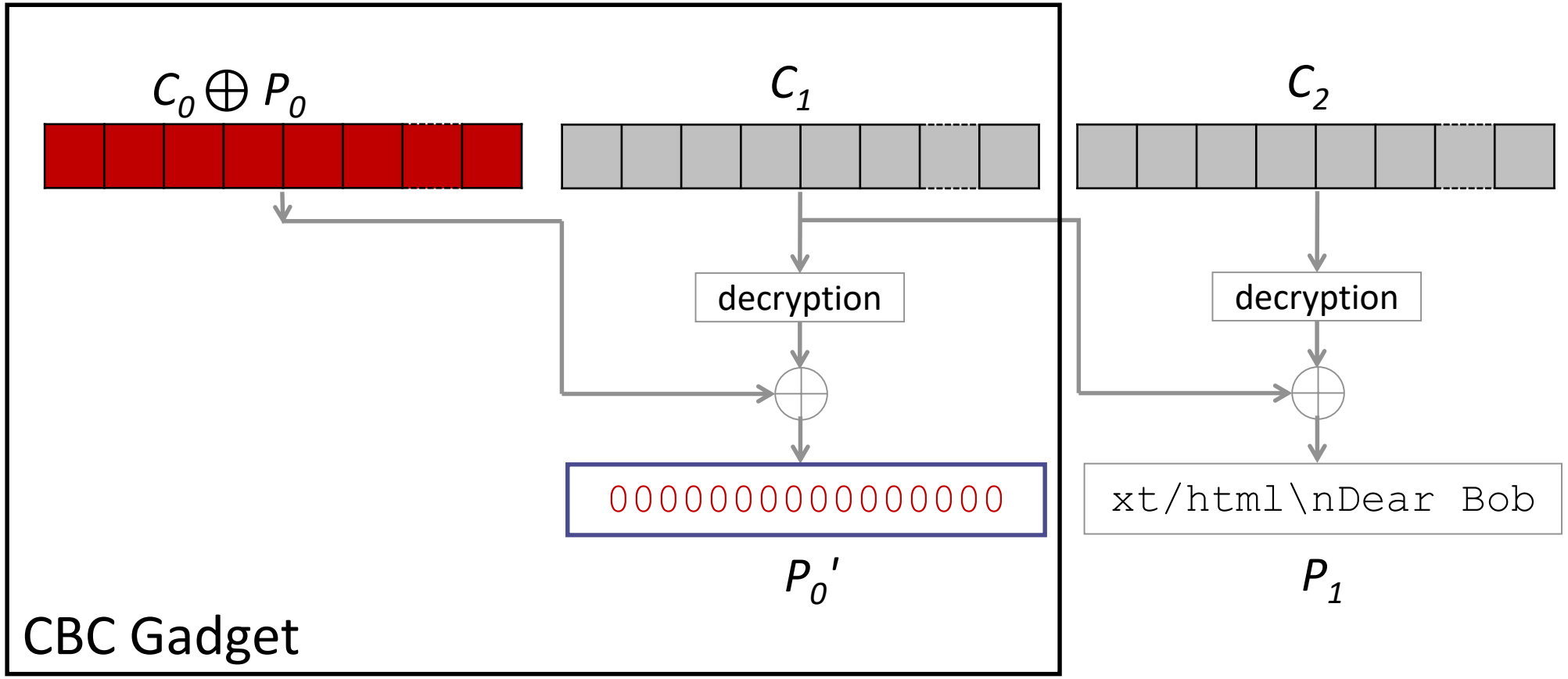
Malleability of CBC



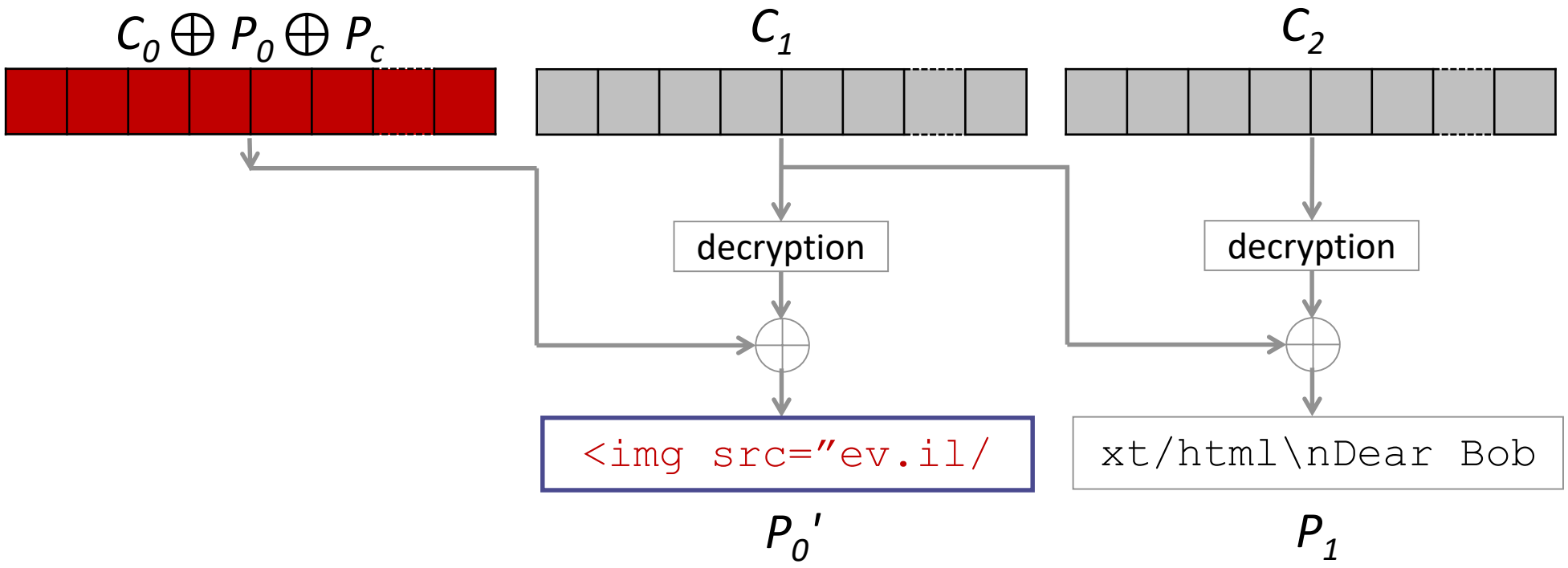
Malleability of CBC



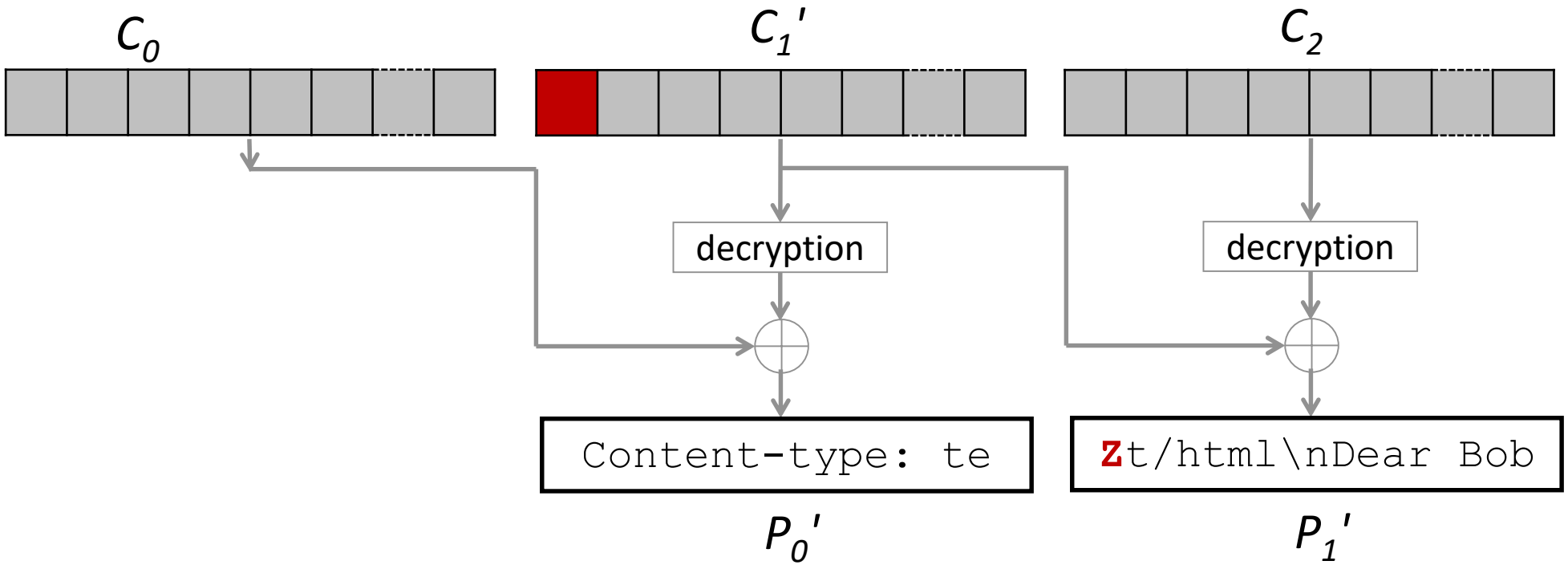
Malleability of CBC



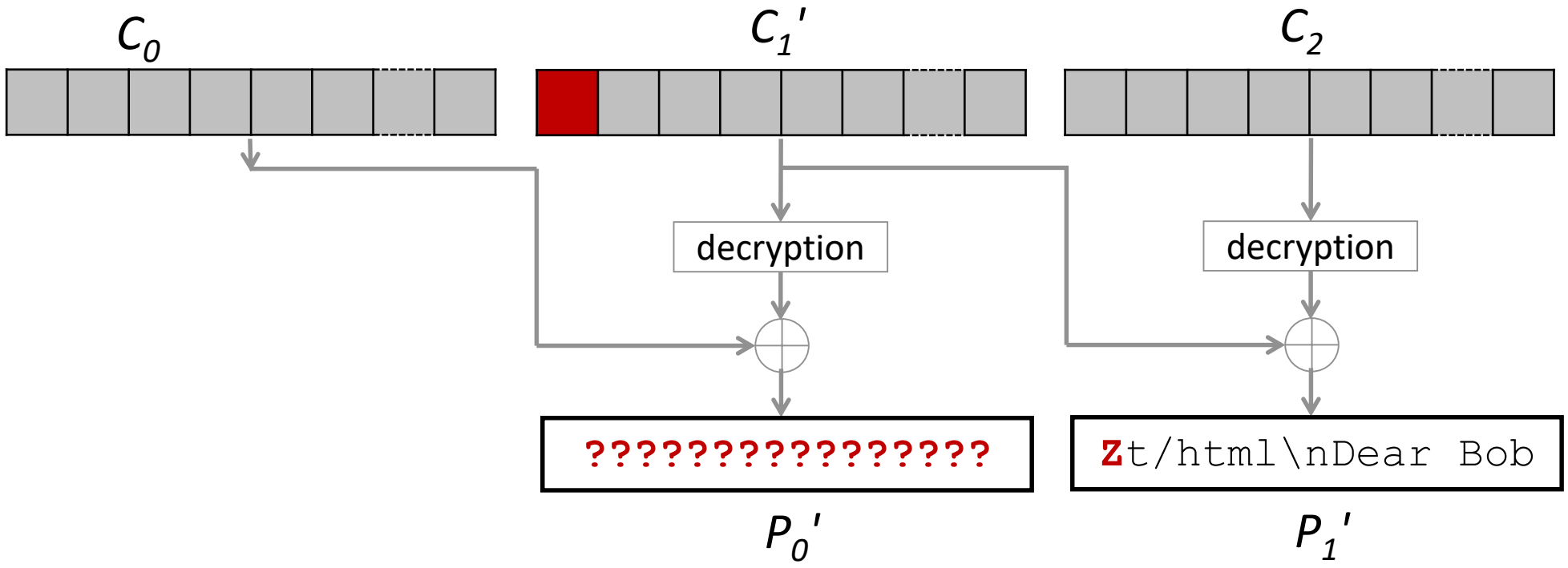
Malleability of CBC



Malleability of CBC



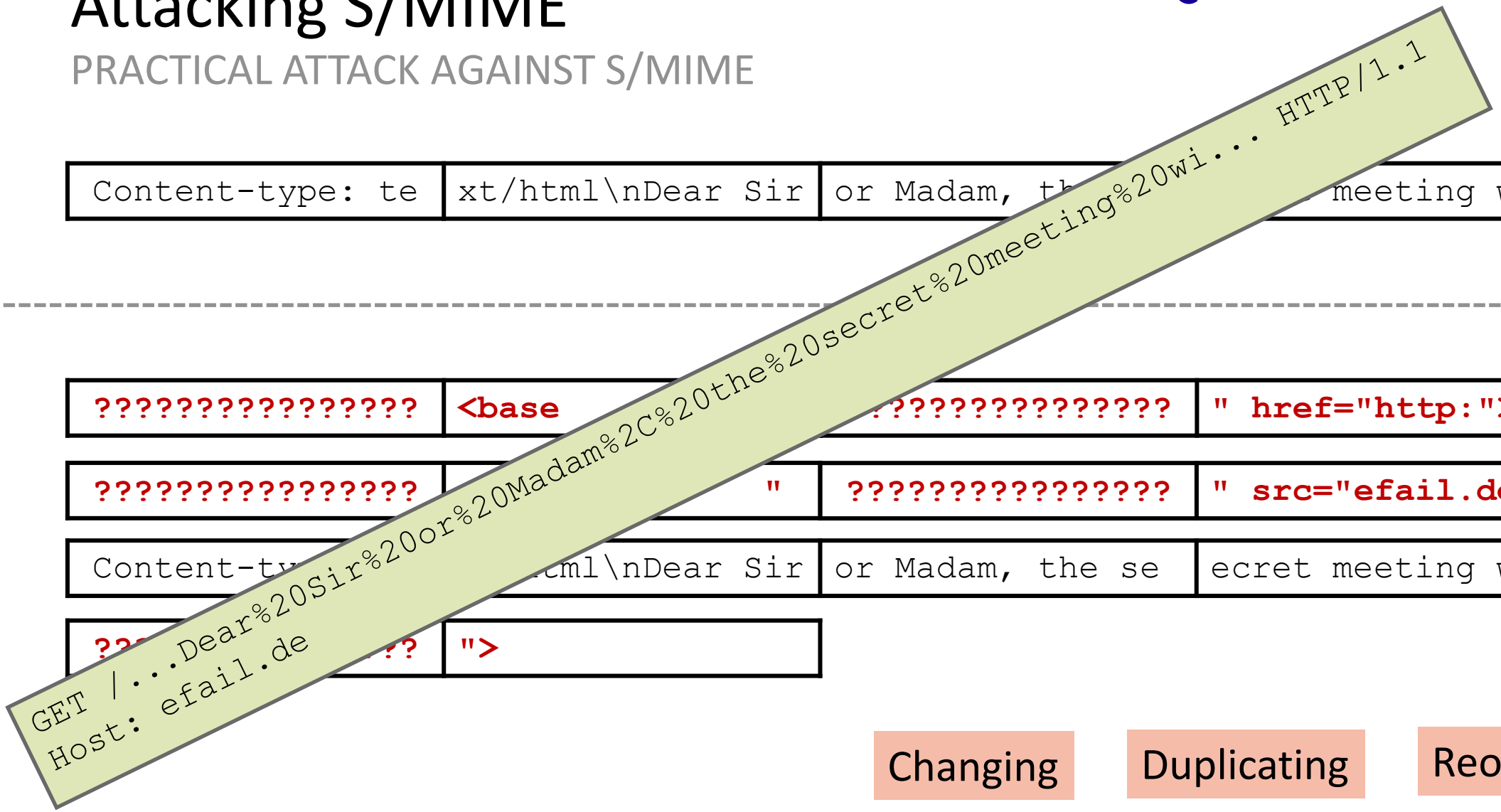
Malleability of CBC



Attacking S/MIME

Attacking S/MIME

PRACTICAL ATTACK AGAINST S/MIME



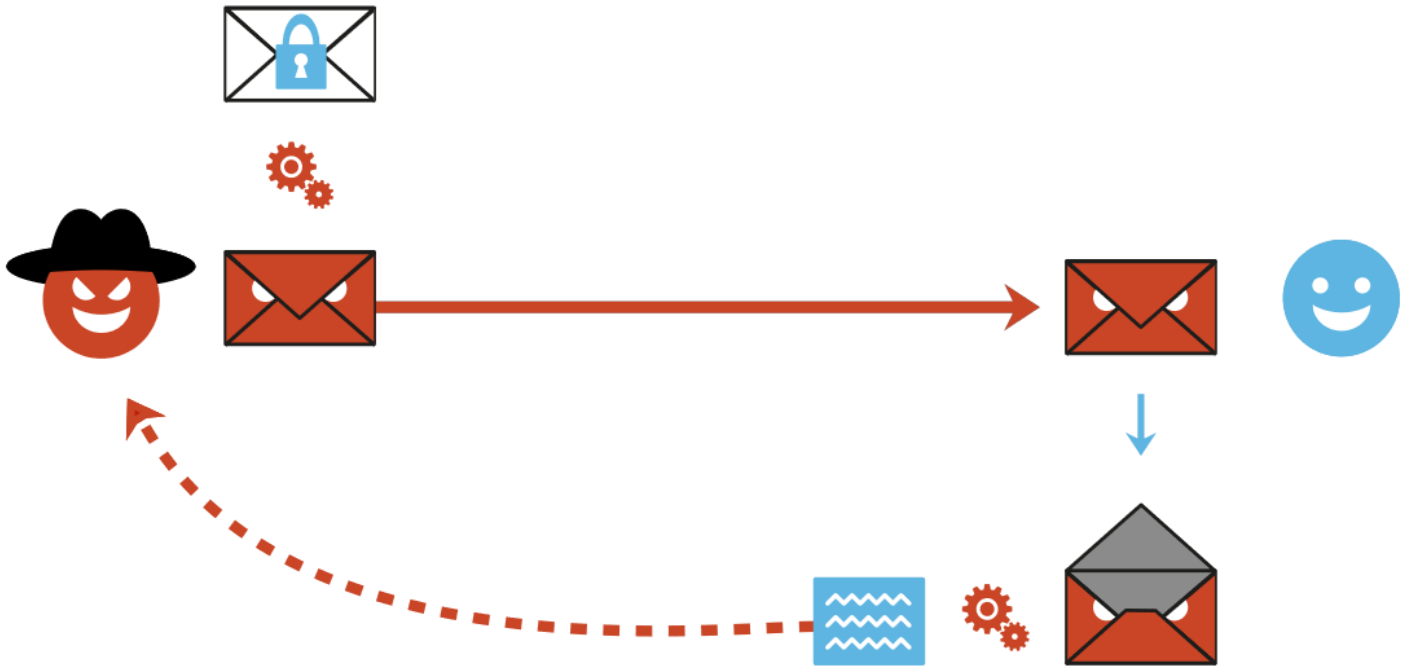
Changing

Duplicating

Reordering

Practical attack against S/MIME

ATTACKER MODEL

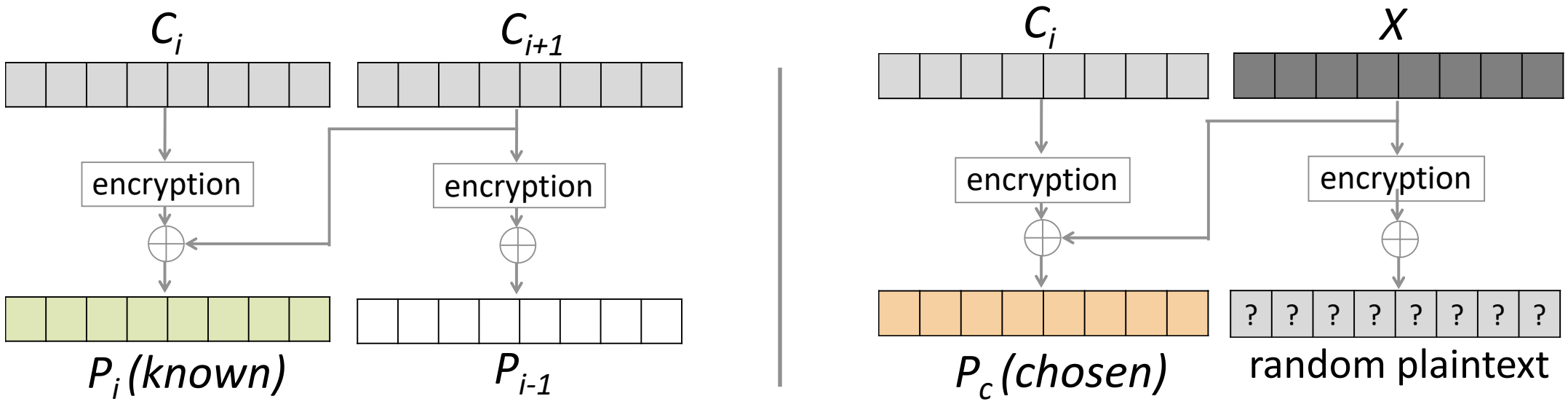


OpenPGP

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			
[illegible]	[illegible]			
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

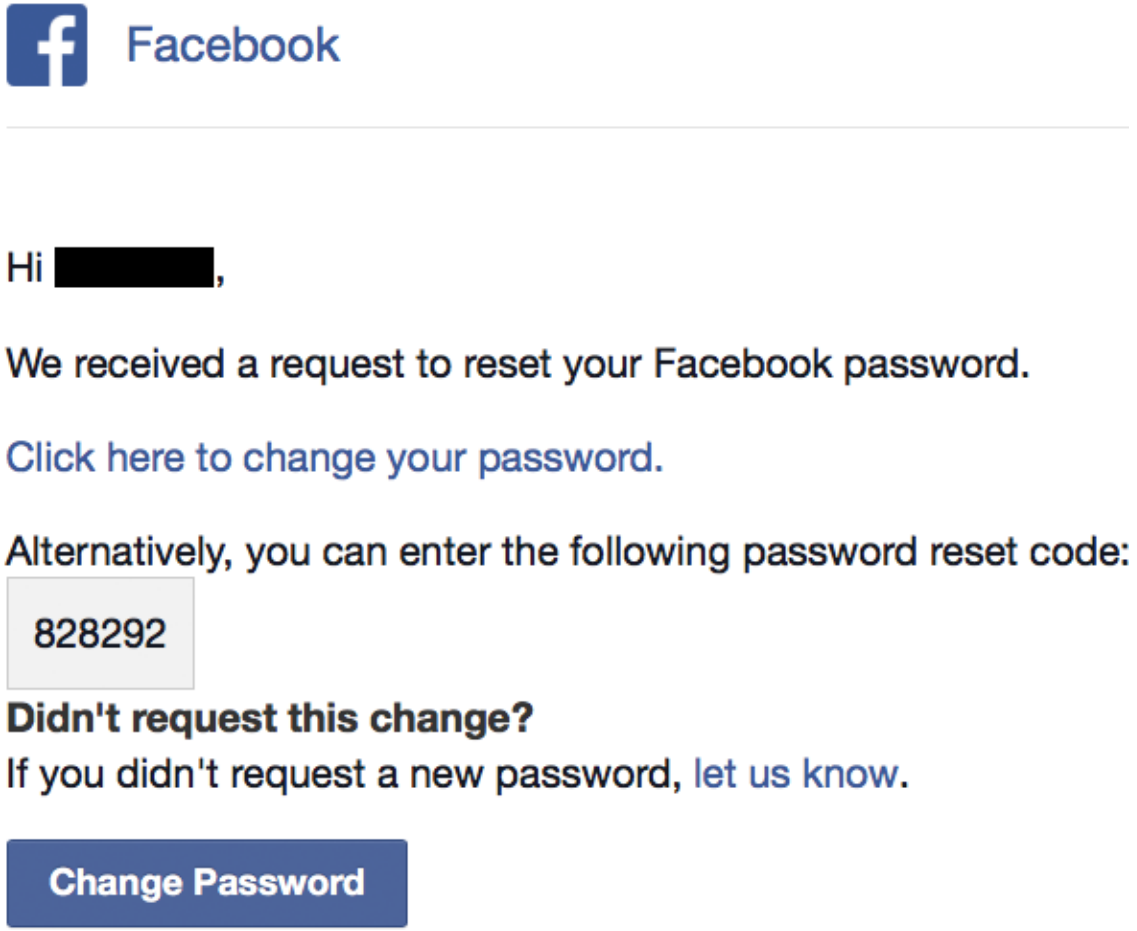
- 211 guesses to break every email

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



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

FH MÜNSTER
University of Applied Sciences

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/