OWASP German Chapter

FH MÜNSTER
University of Applied Sciences

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

FH MÜNSTER
University of Applied Sciences

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

FH MÜNSTER
University of Applied Sciences

OpenPGP (RFC 4880)

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

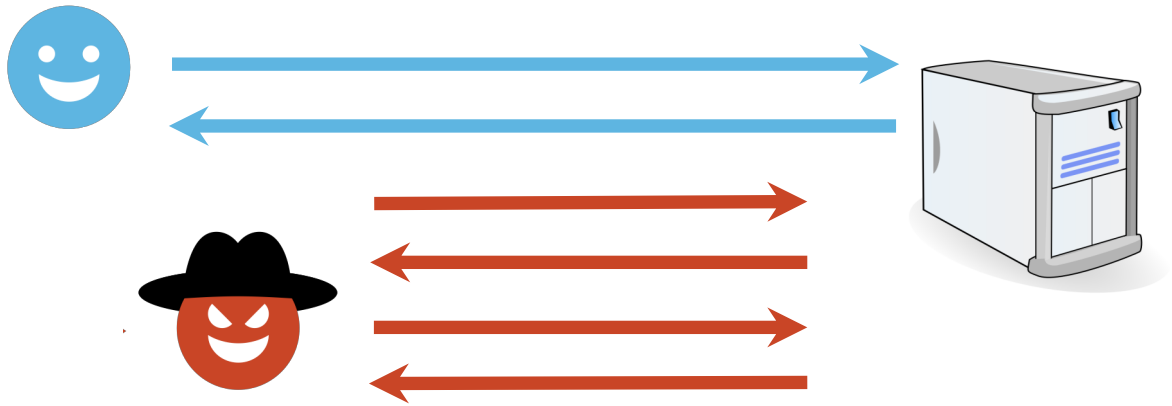
S/MIME (RFC 5751)

- Favored by organizations
- Multi root trust hierarchies

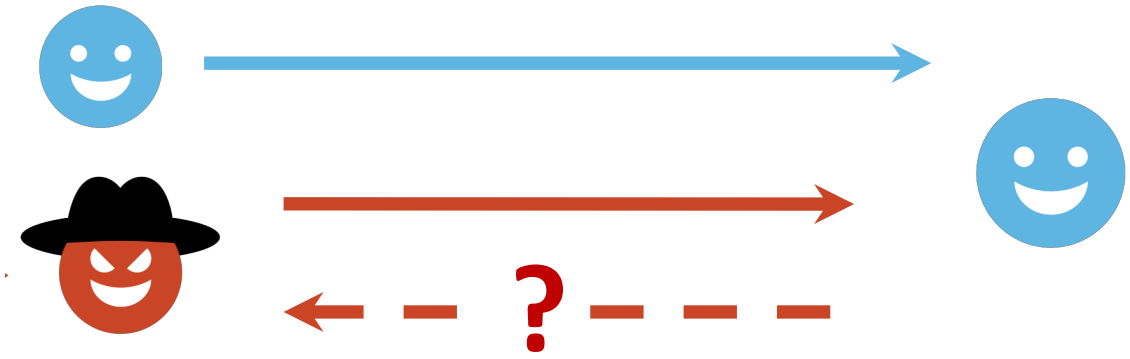
Security of email encryption

FH MÜNSTER
University of Applied Sciences

Request/response protocols



Email is non-interactive



Backchannel techniques

FH MÜNSTER
University of Applied Sciences

Forcing an email client to send responses via *backchannels*

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

```
<img src="http://efail.de">
<object data="ftp://efail.de">
<style>@import '//efail.de'</style>
...
```

Backchannel techniques

FH MÜNSTER
University of Applied Sciences

Forcing an email client to send responses via *backchannels*

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

Disposition-Notification-To: eve@evil.com
Remote-Attachment-URL: http://efail.de
X-Image-URL: http://efail.de
…

Backchannel techniques

FH MÜNSTER
University of Applied Sciences

Forcing an email client to send responses via *backchannels*

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

PDF, SVG, VCards, etc.

Backchannel techniques

FH MÜNSTER
University of Applied Sciences

Forcing an email client to send responses via *backchannels*

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

OCSP, CRL, intermediate certs

Evaluation of backchannels in email clients

FH MÜNSTER
University of Applied Sciences

Windows	Outlook	Postbox	Live Mail	The Bat!	eM Client	W8Mail
	IBM Notes	Foxmail	Pegasus	Mulberry	WLMail	W10Mail
Linux	Thunderbird	KMail	Claws			
	Evolution	Trojitá	Mutt			
macOS	Apple Mail	Airmail	MailMate			
iOS	Mail App	CanaryMail	Outlook			
Android	K-9 Mail	MailDroid				
	R2Mail	Nine				
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			

User interaction

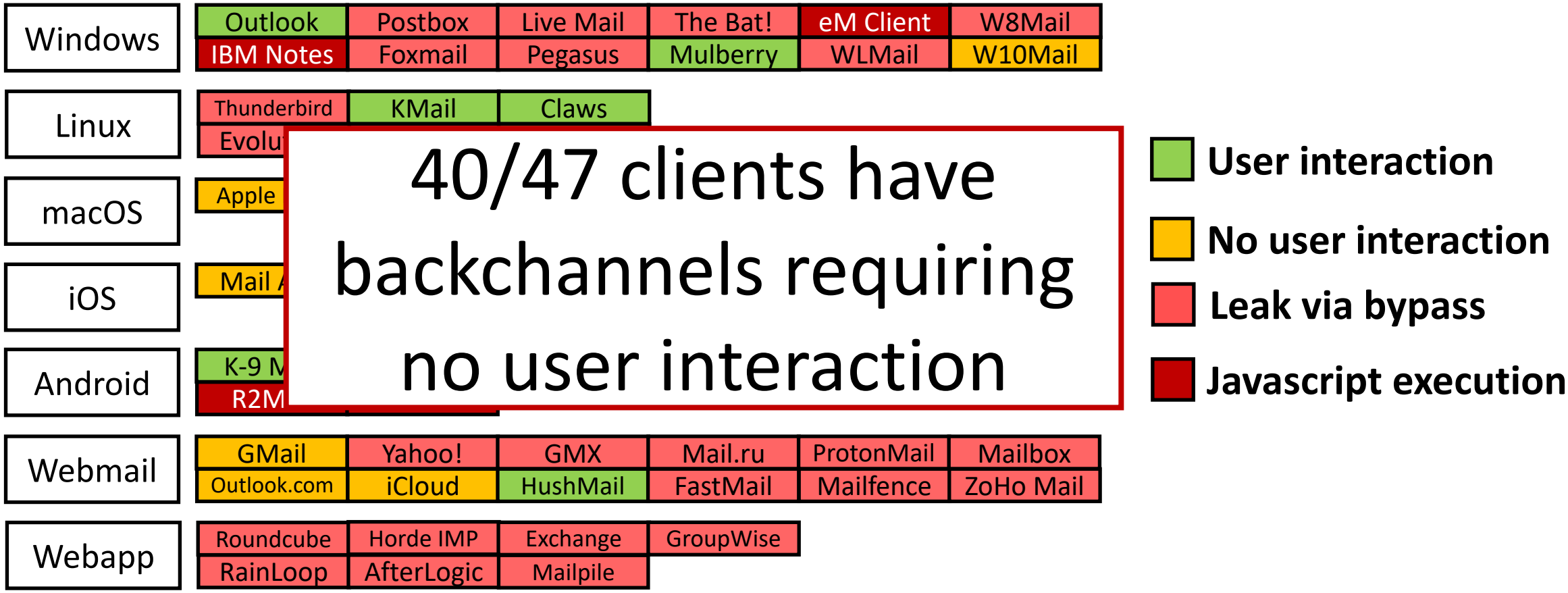
No user interaction

Leak via bypass

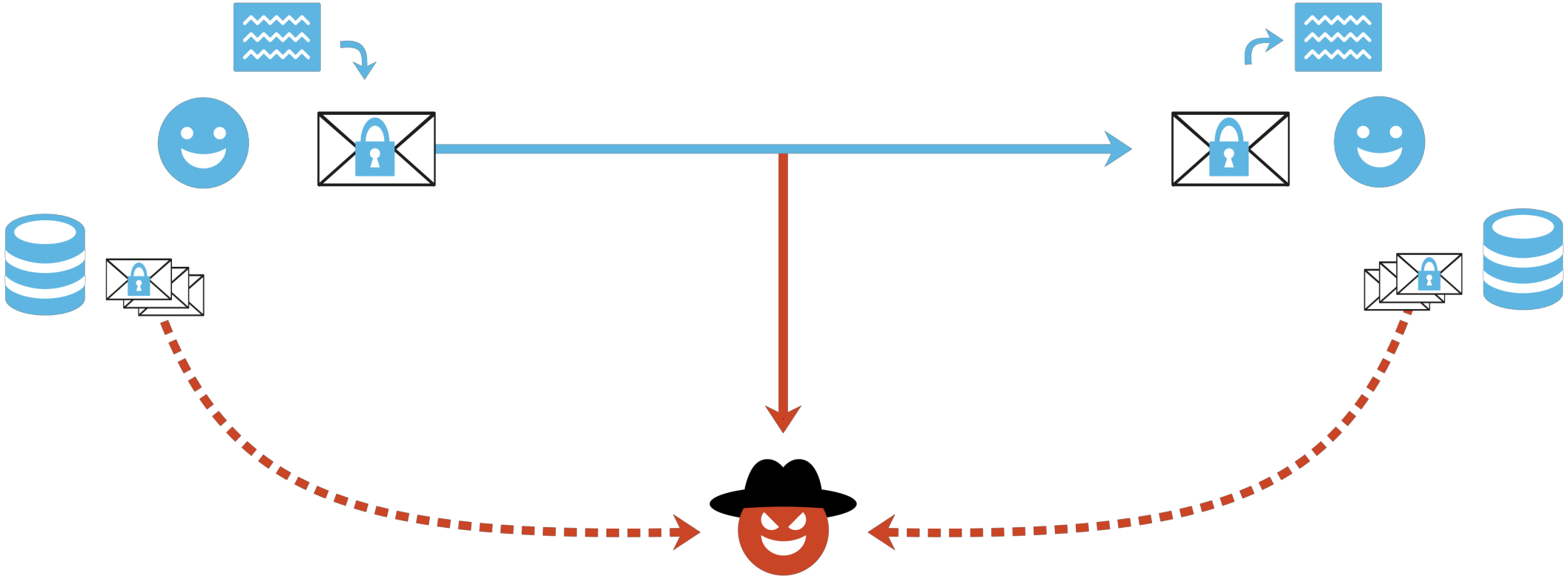
Javascript execution

Evaluation of backchannels in email clients

FH MÜNSTER
University of Applied Sciences

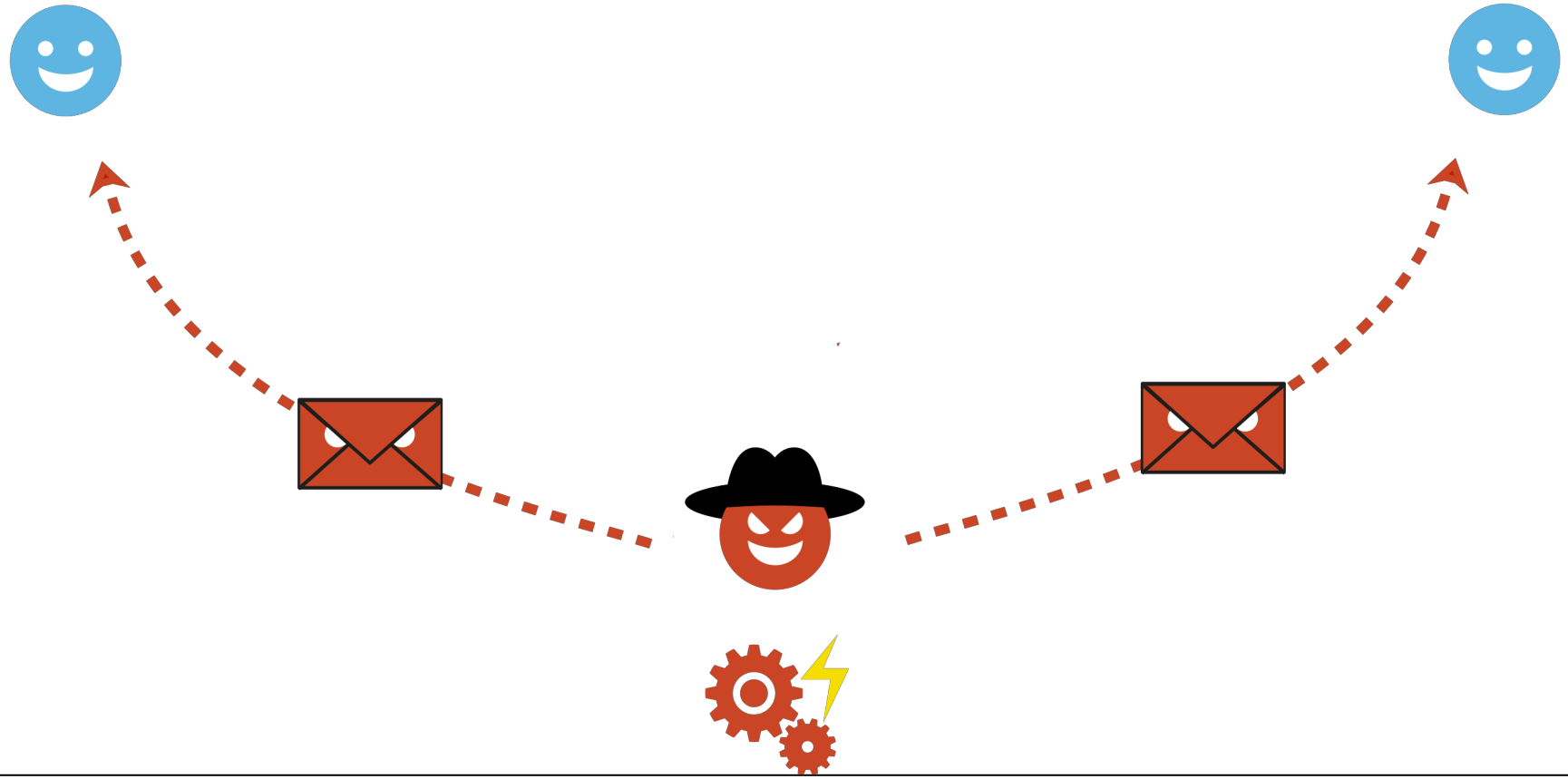


Attacker model



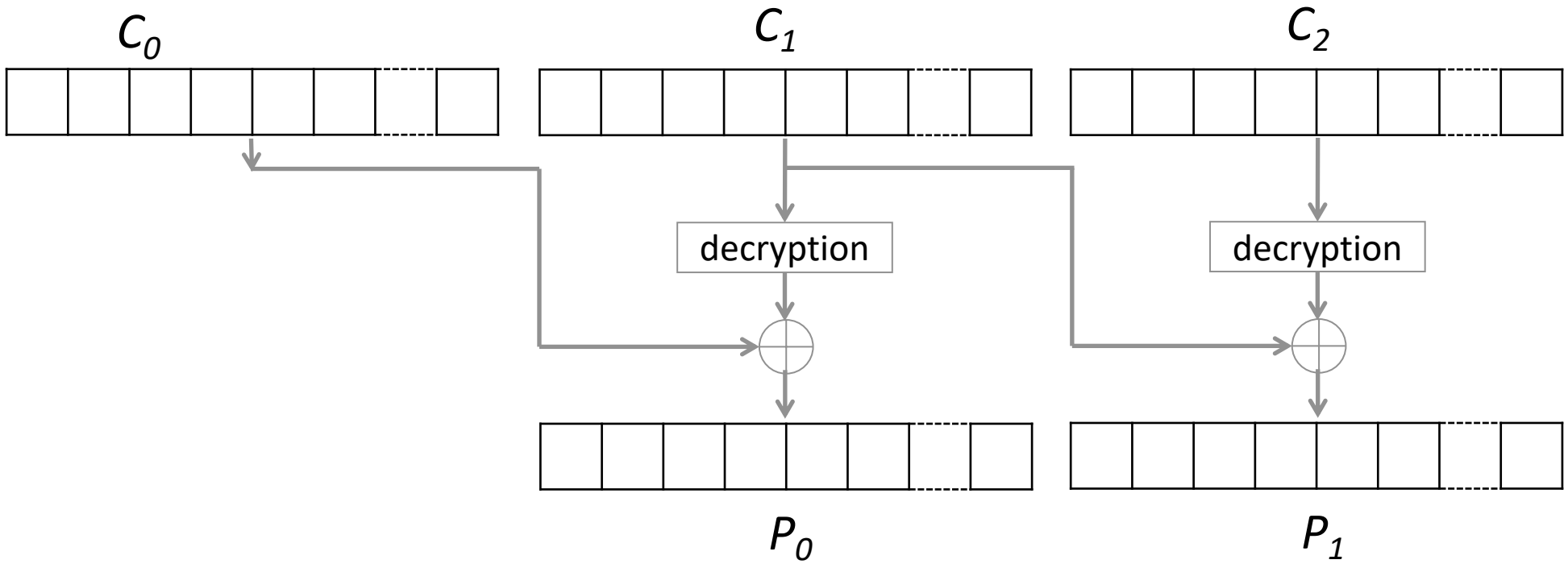
Attacker model

FH MÜNSTER
University of Applied Sciences

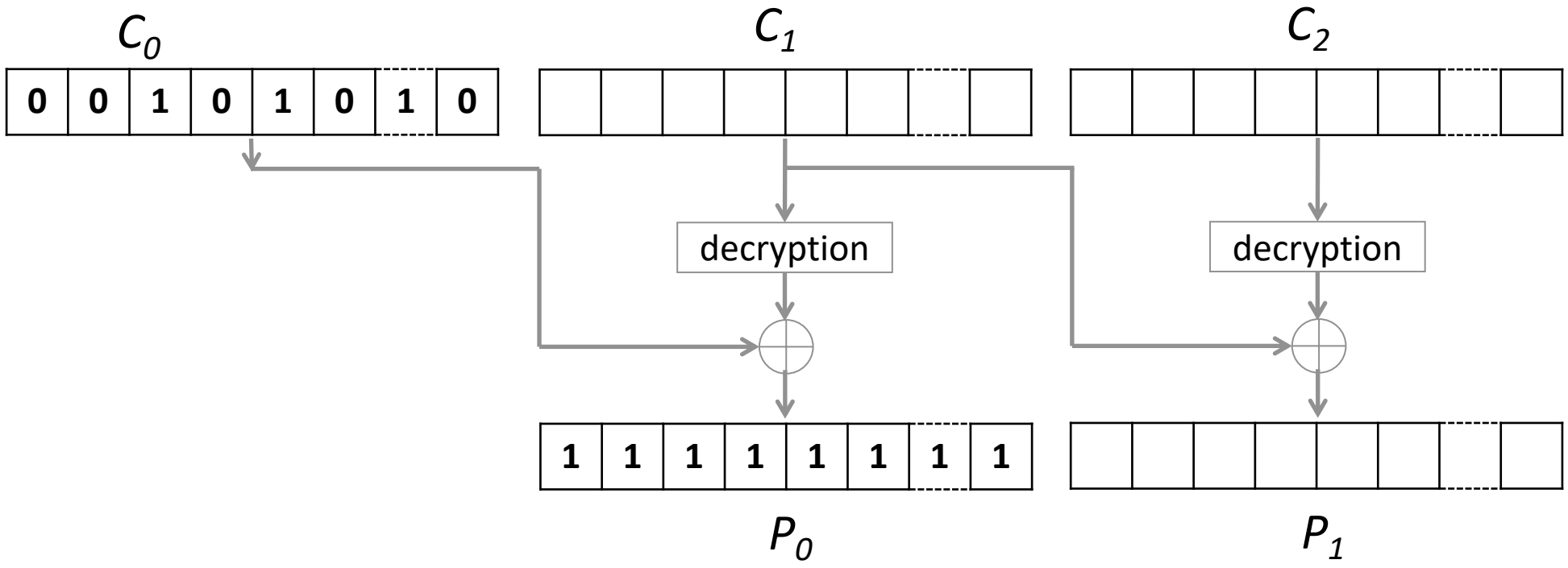


S/MIME

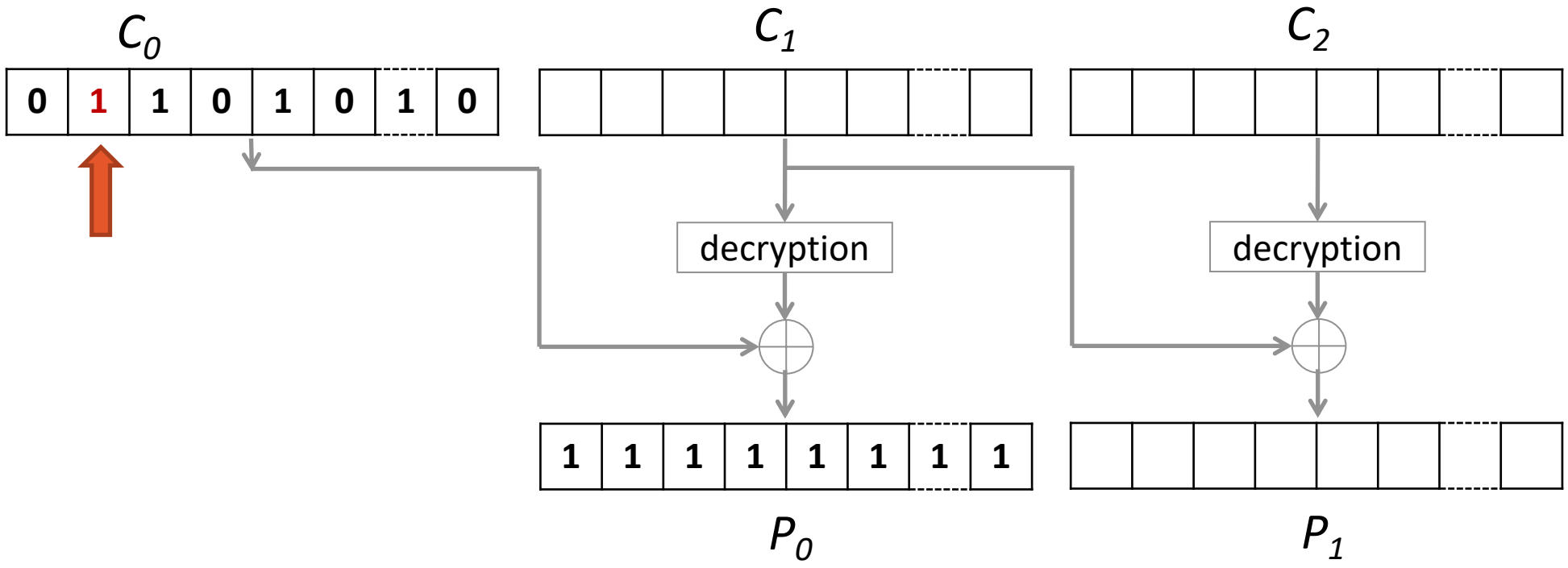
Malleability of CBC



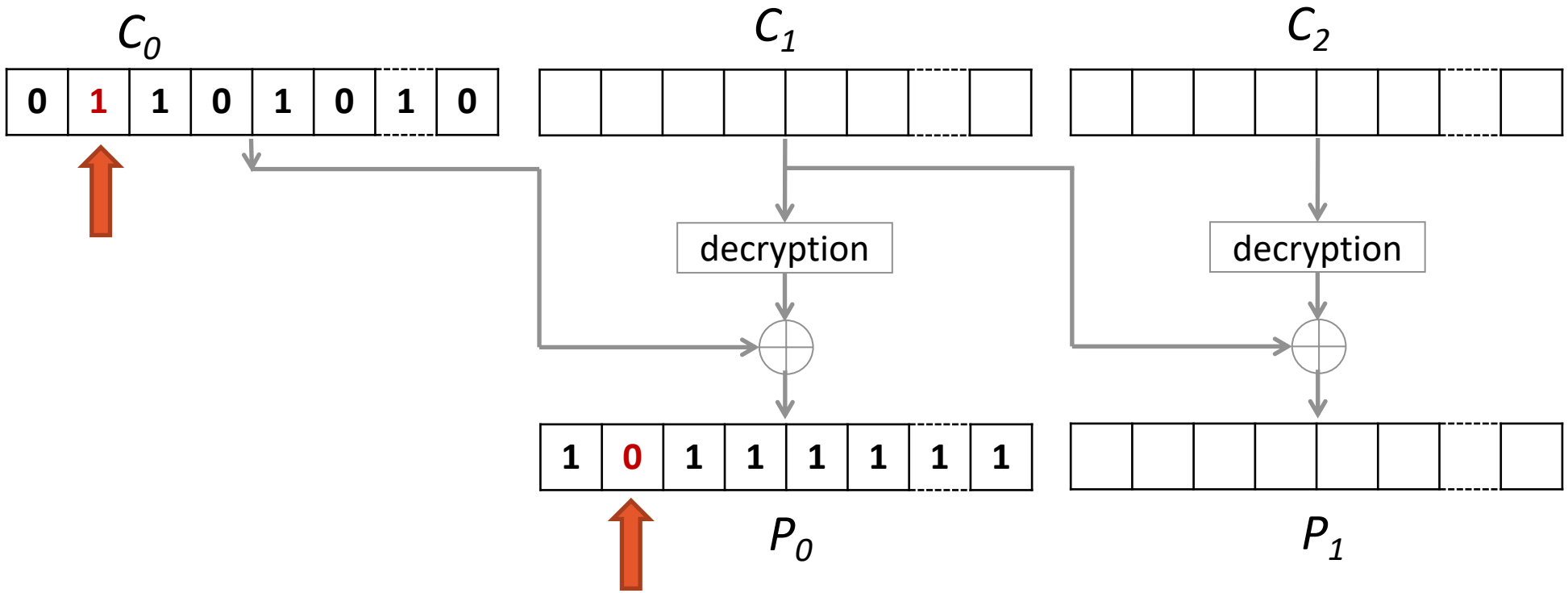
Malleability of CBC



Malleability of CBC

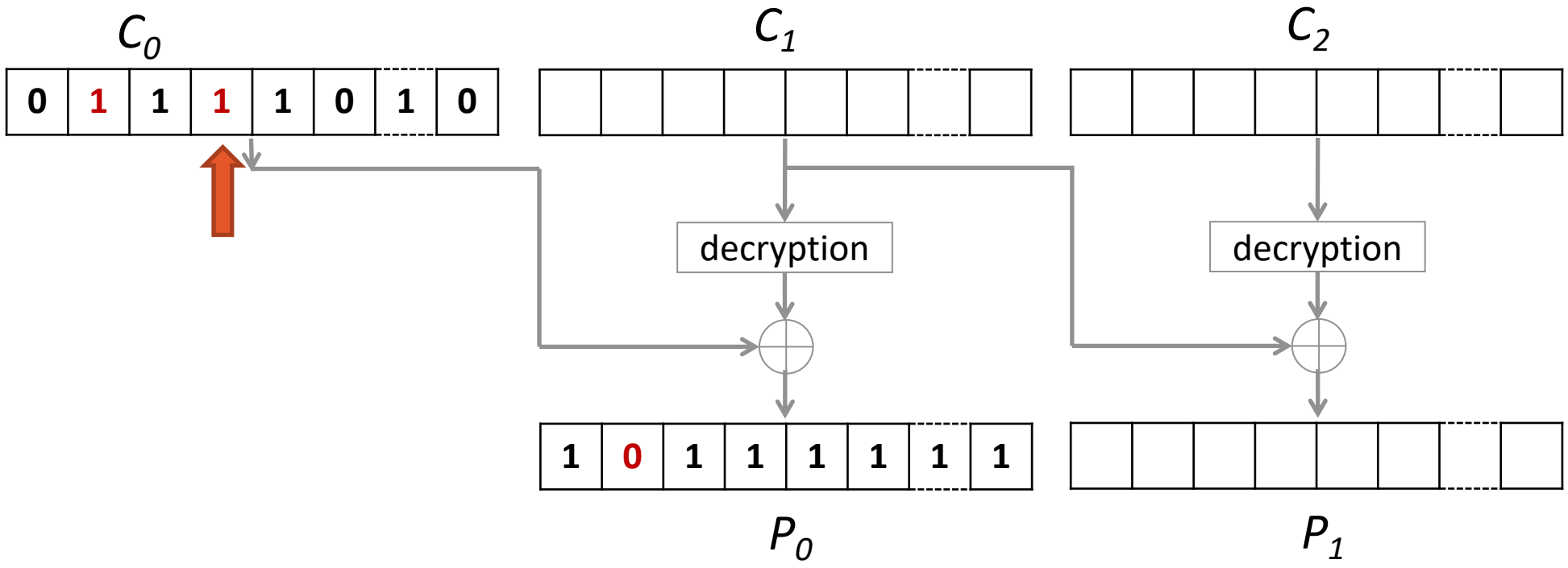


Malleability of CBC

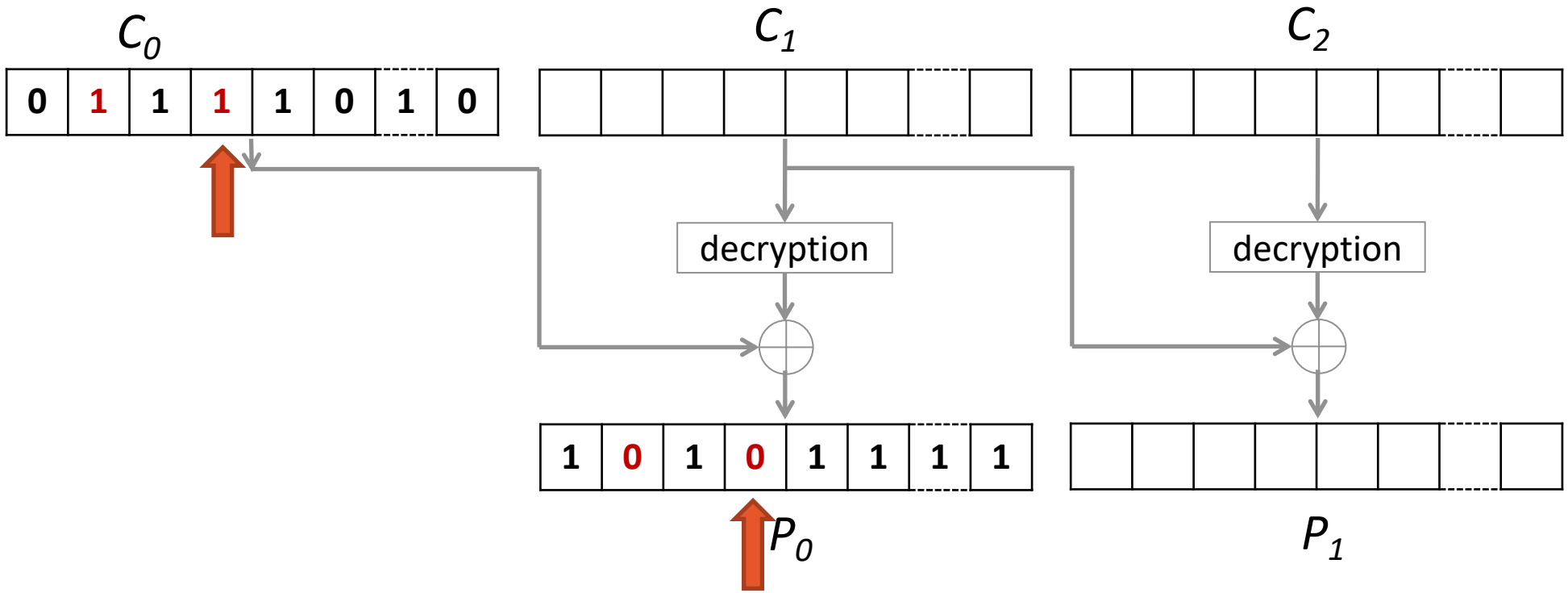


Malleability of CBC

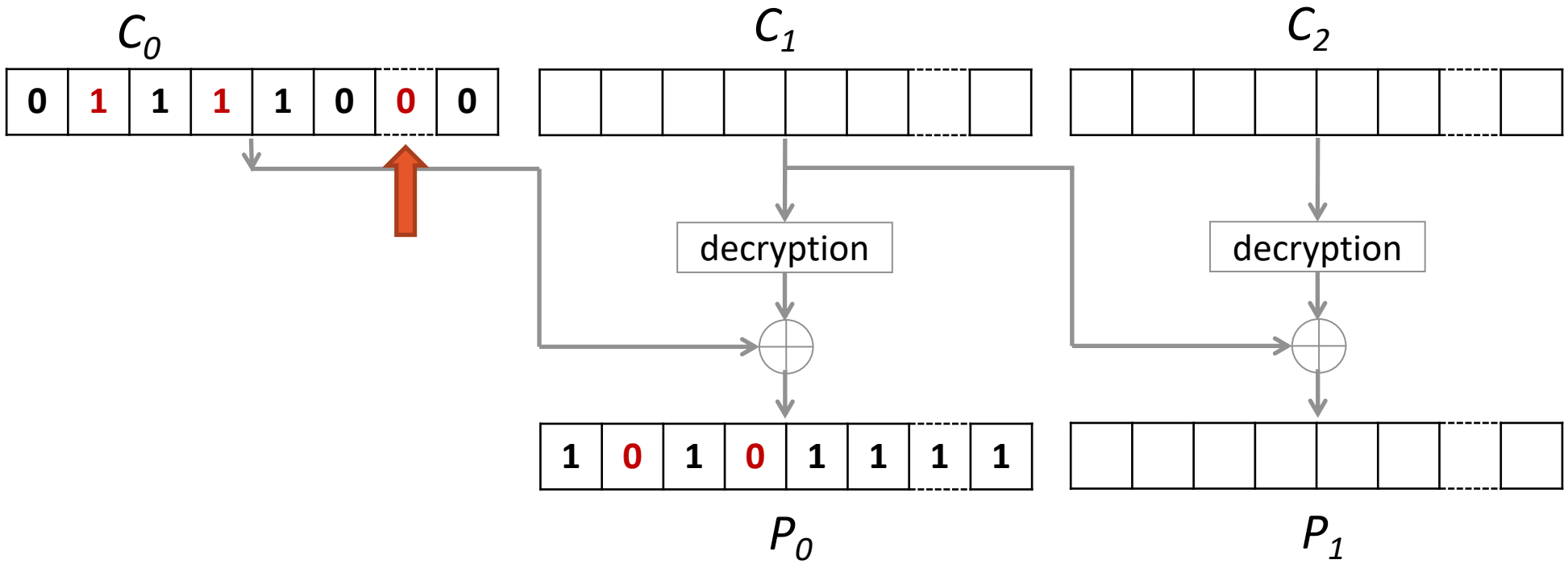
FH MÜNSTER
University of Applied Sciences



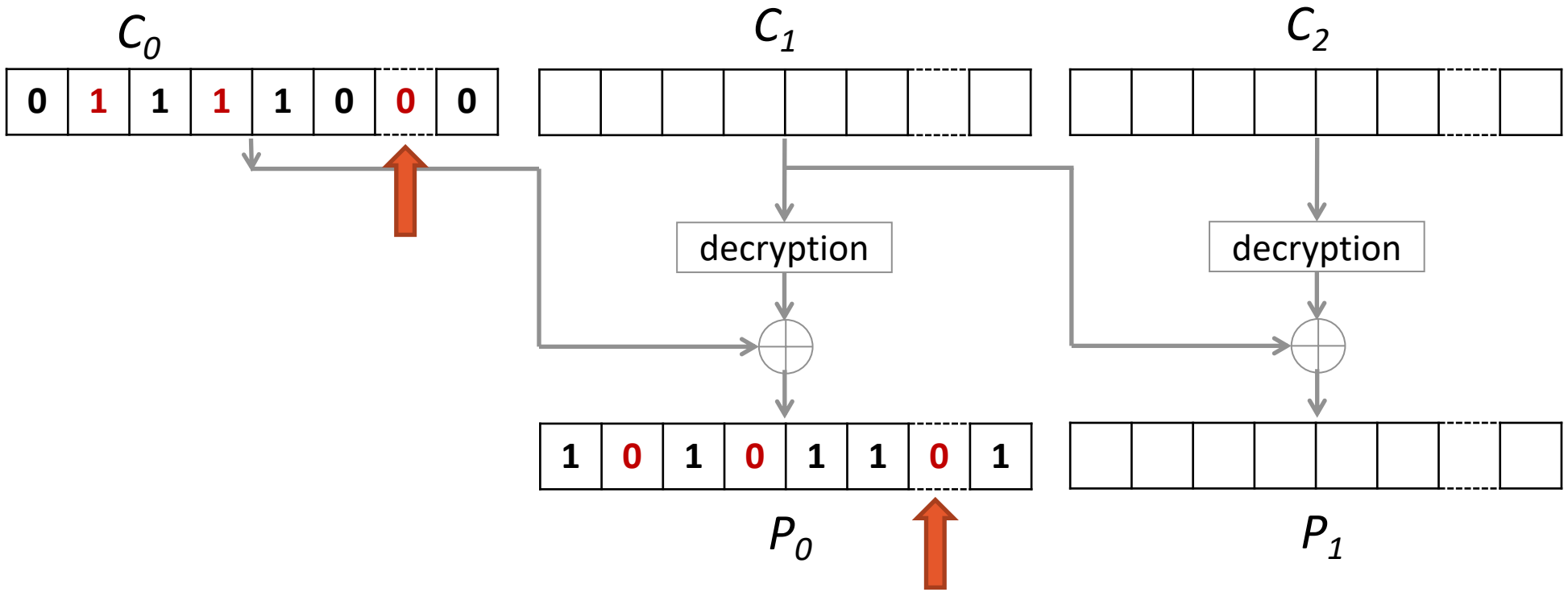
Malleability of CBC



Malleability of CBC

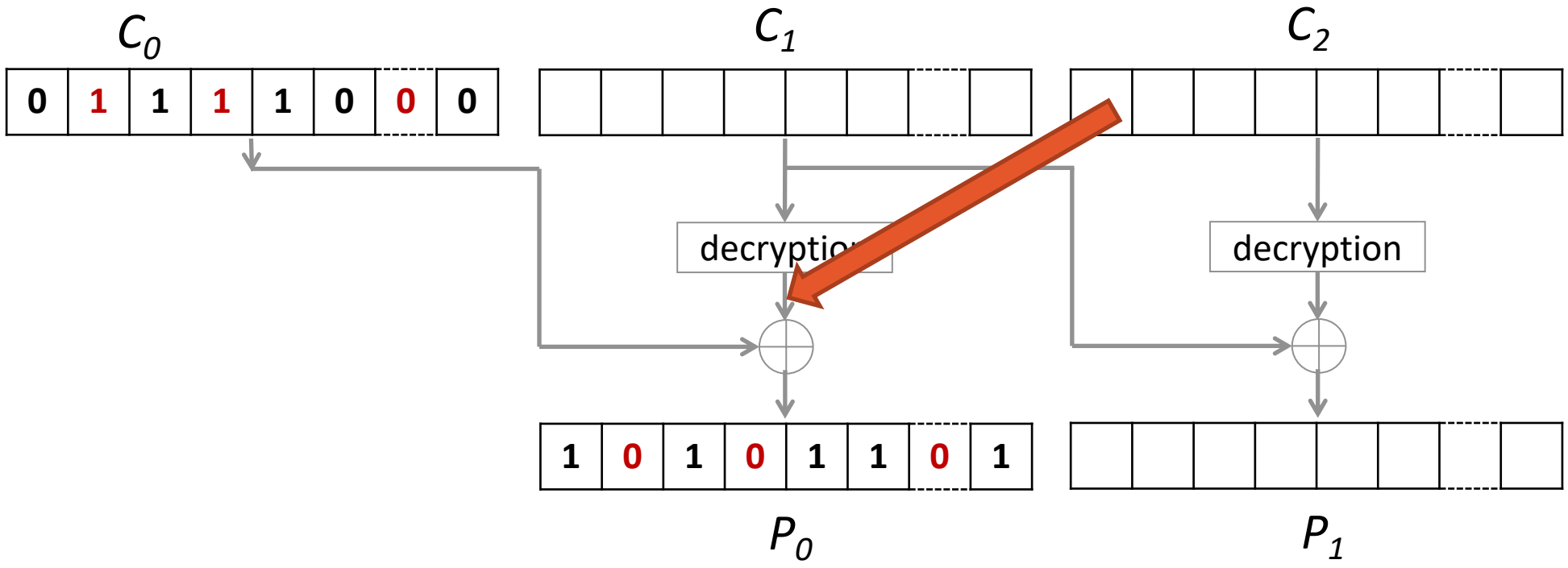


Malleability of CBC

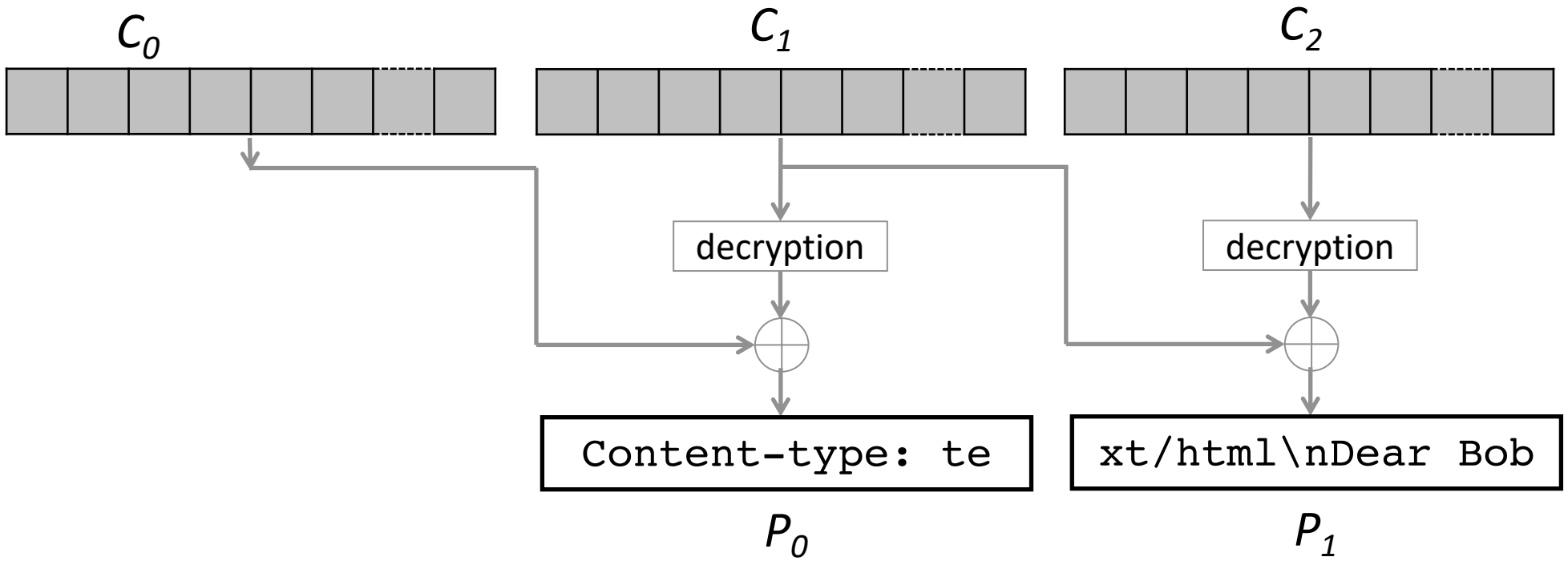


Malleability of CBC

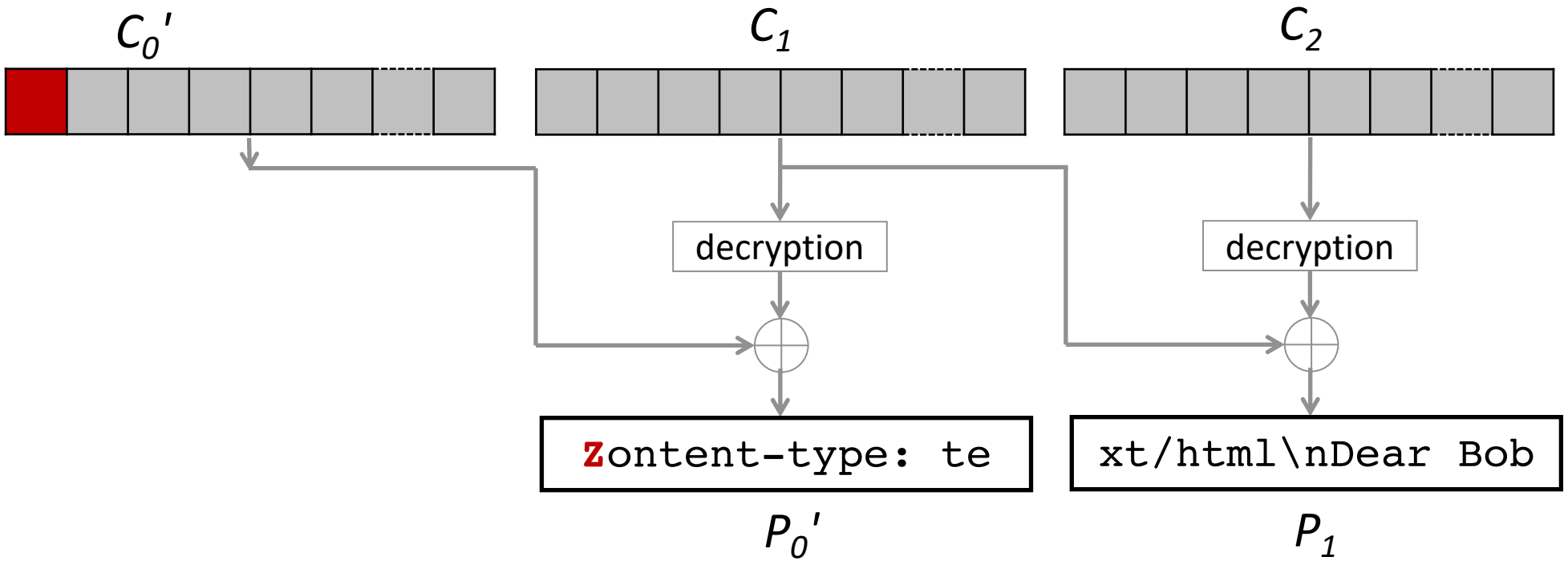
FH MÜNSTER
University of Applied Sciences



Malleability of CBC

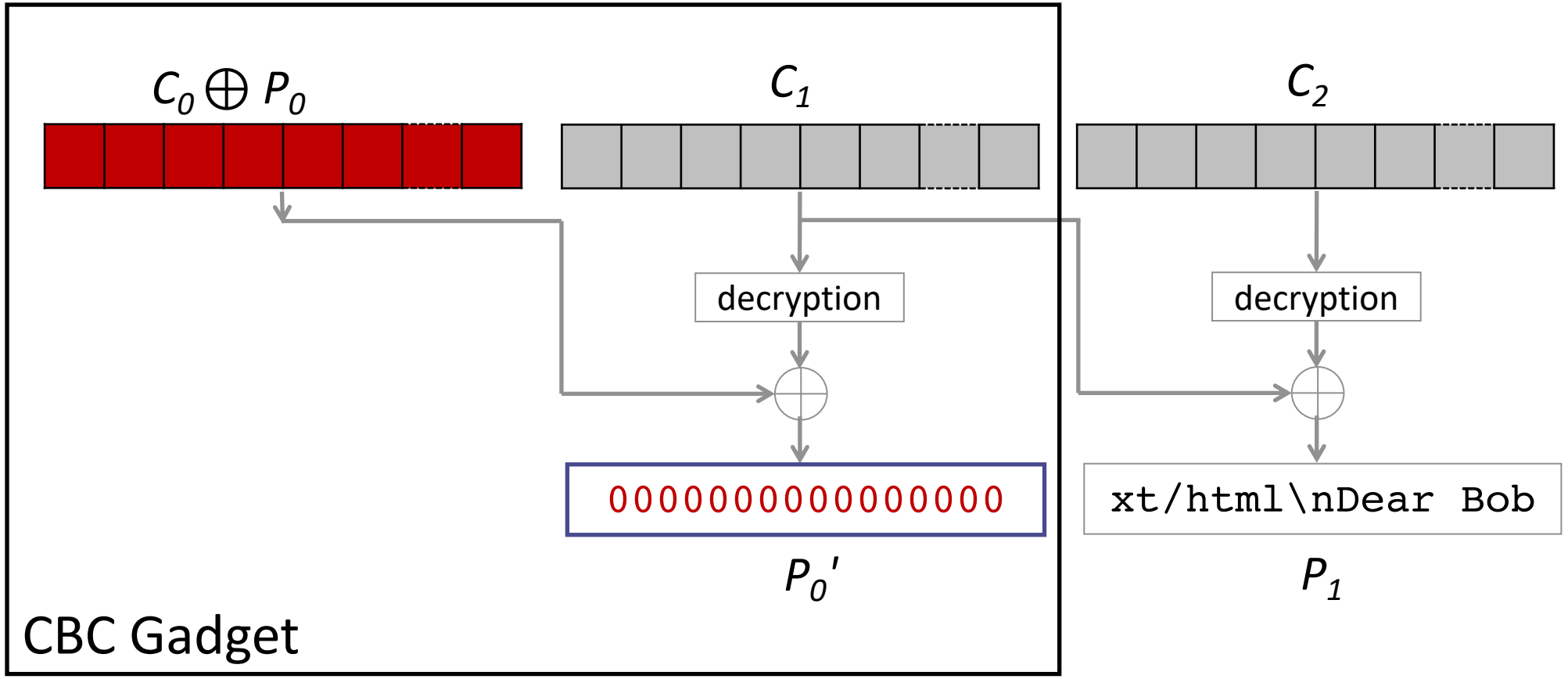


Malleability of CBC

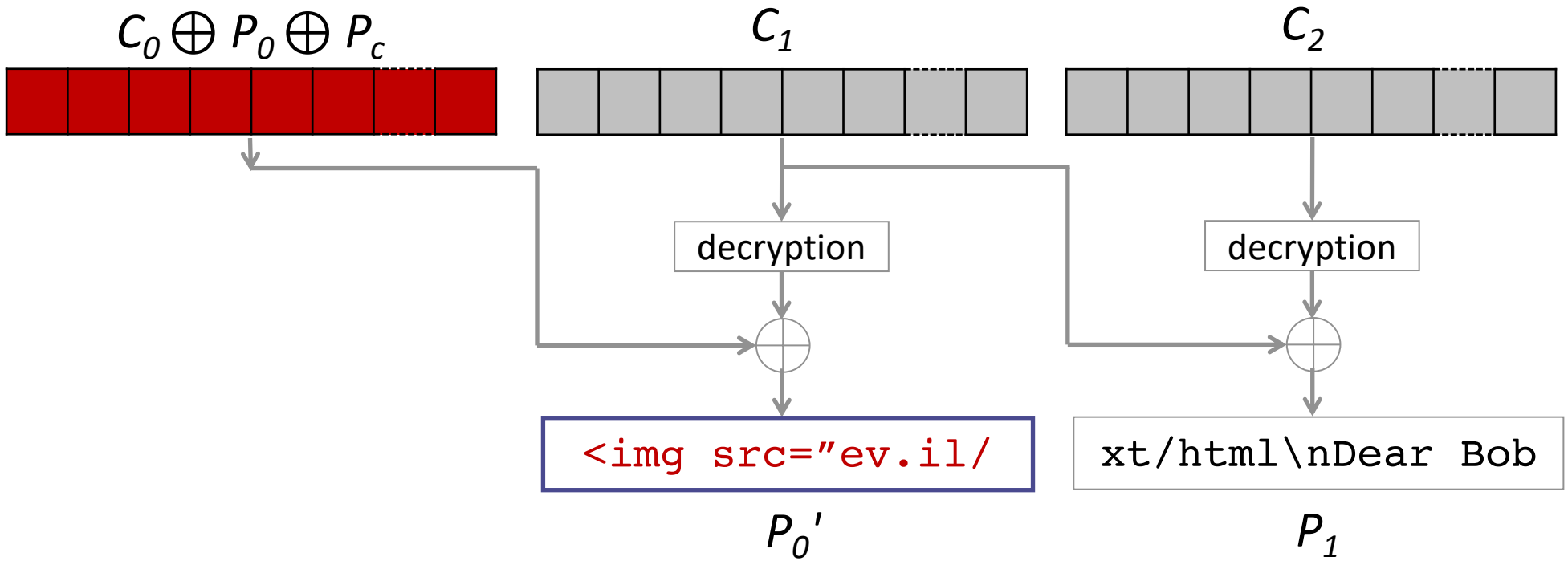


Malleability of CBC

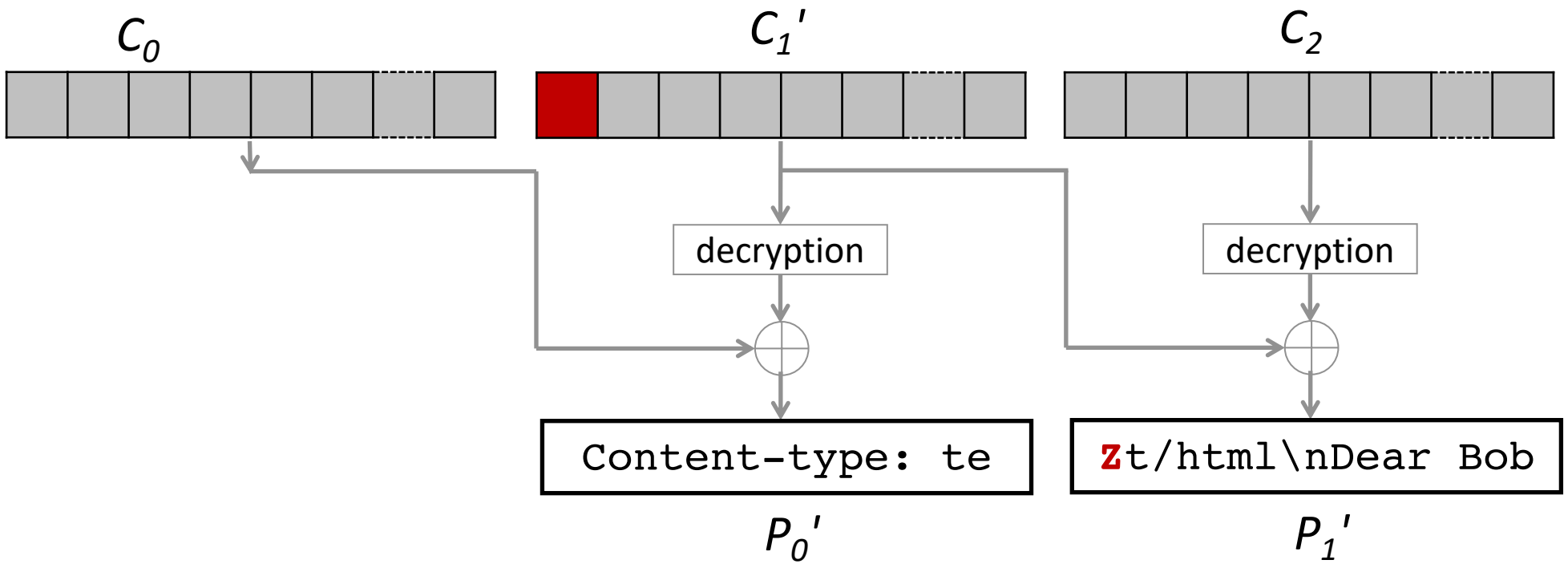
FH MÜNSTER
University of Applied Sciences



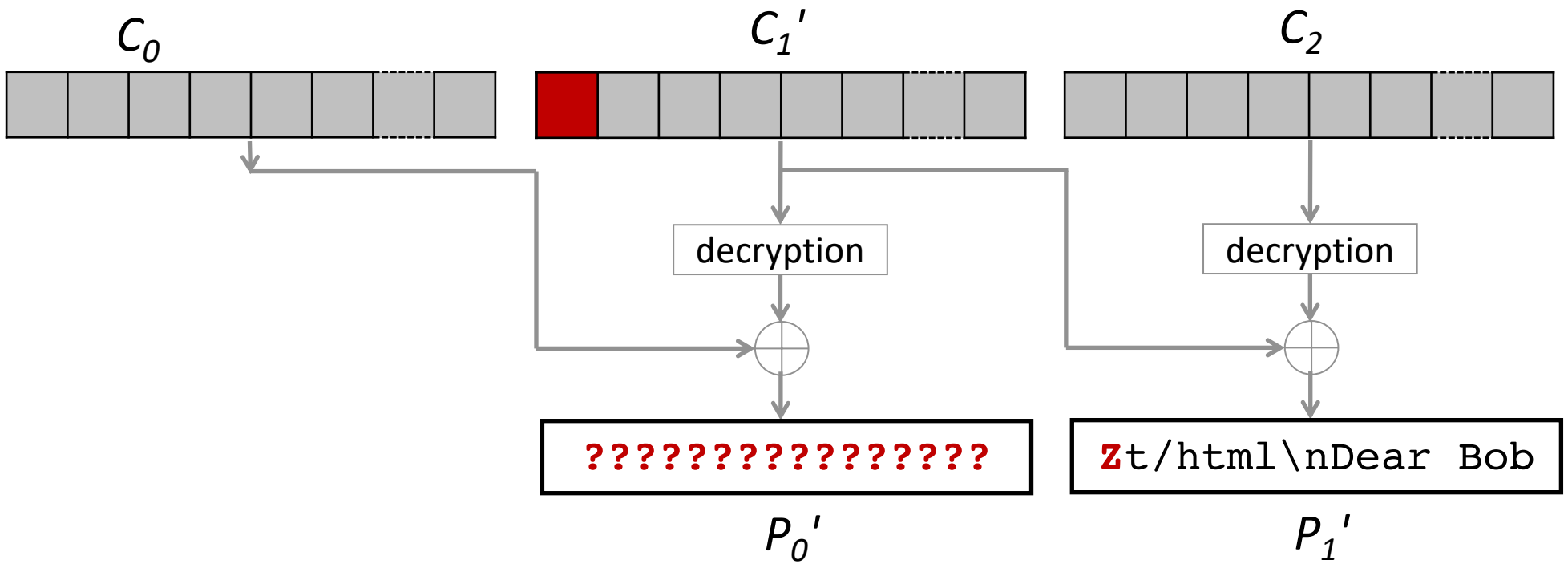
Malleability of CBC



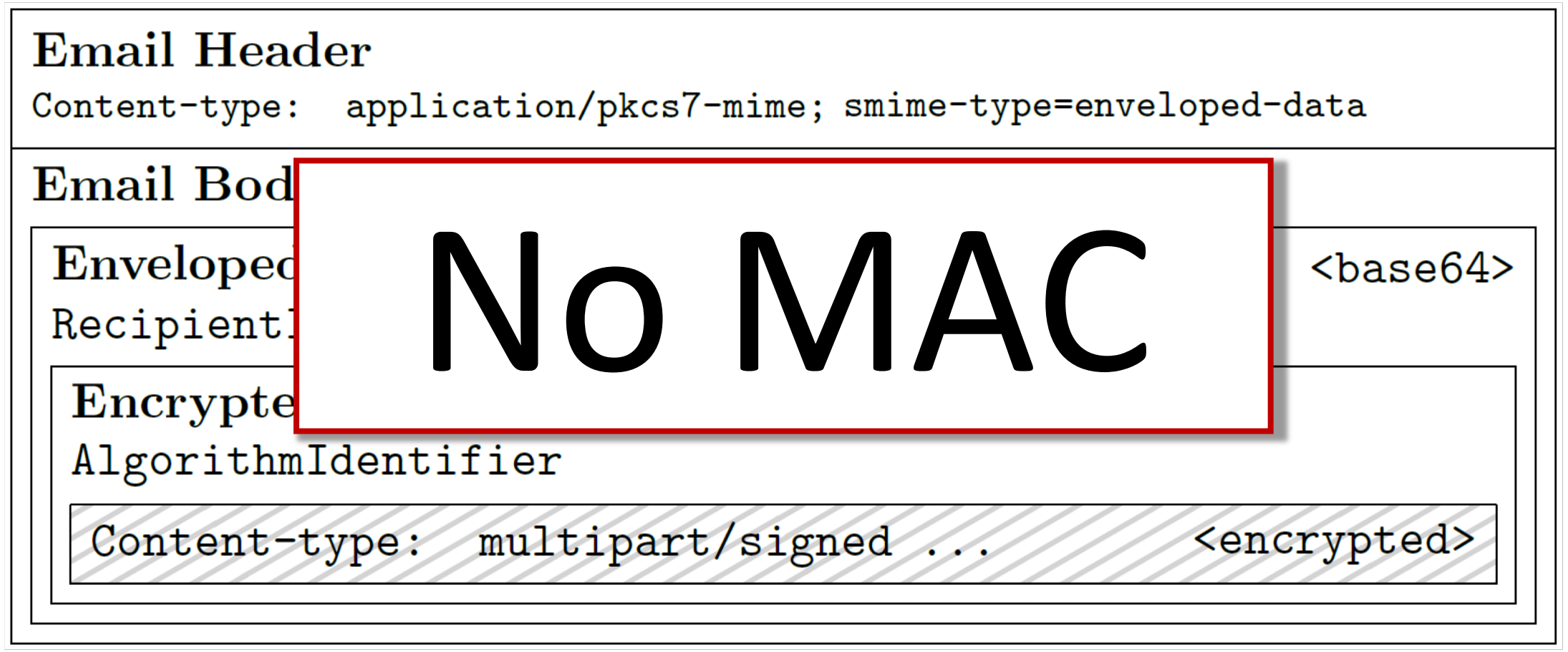
Malleability of CBC



Malleability of CBC

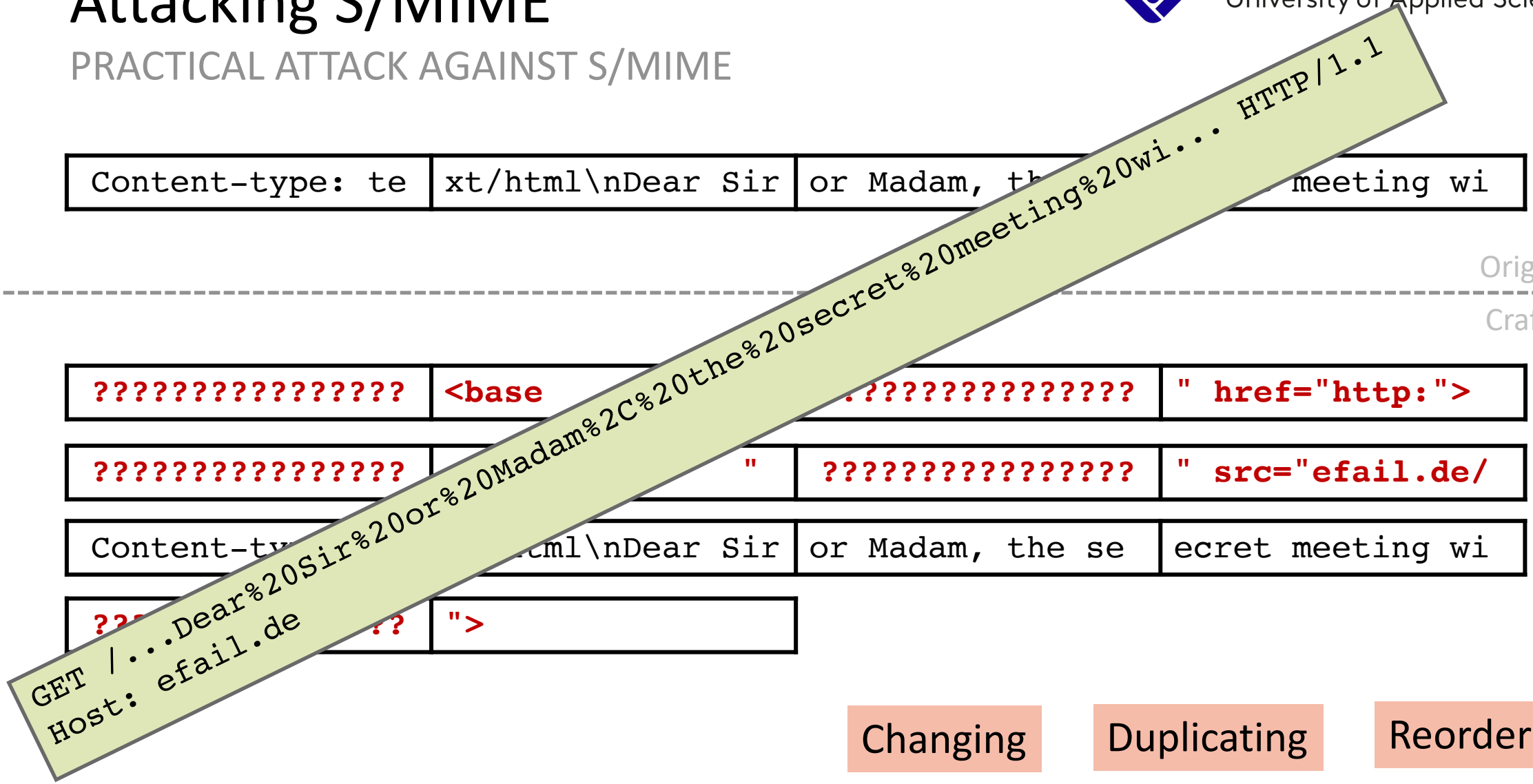


Attacking S/MIME



Attacking S/MIME

PRACTICAL ATTACK AGAINST S/MIME



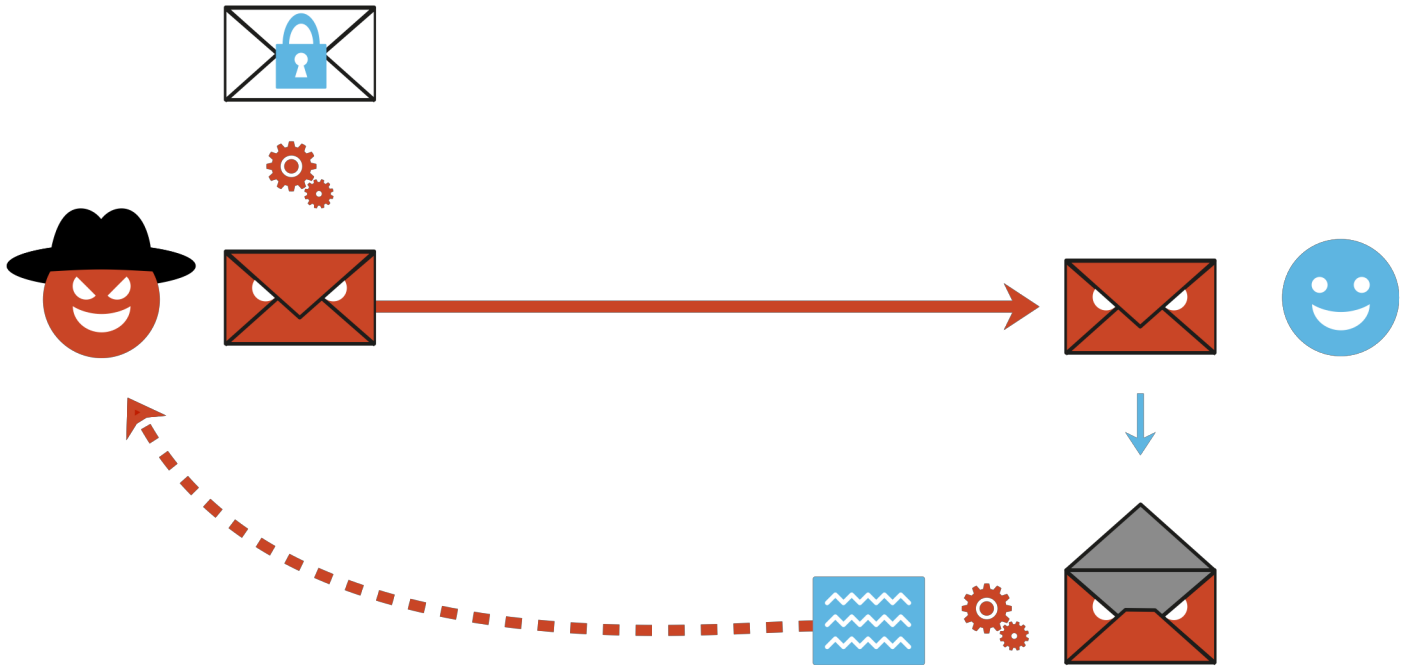
Changing

Duplicating

Reordering

Practical attack against S/MIME

ATTACKER MODEL



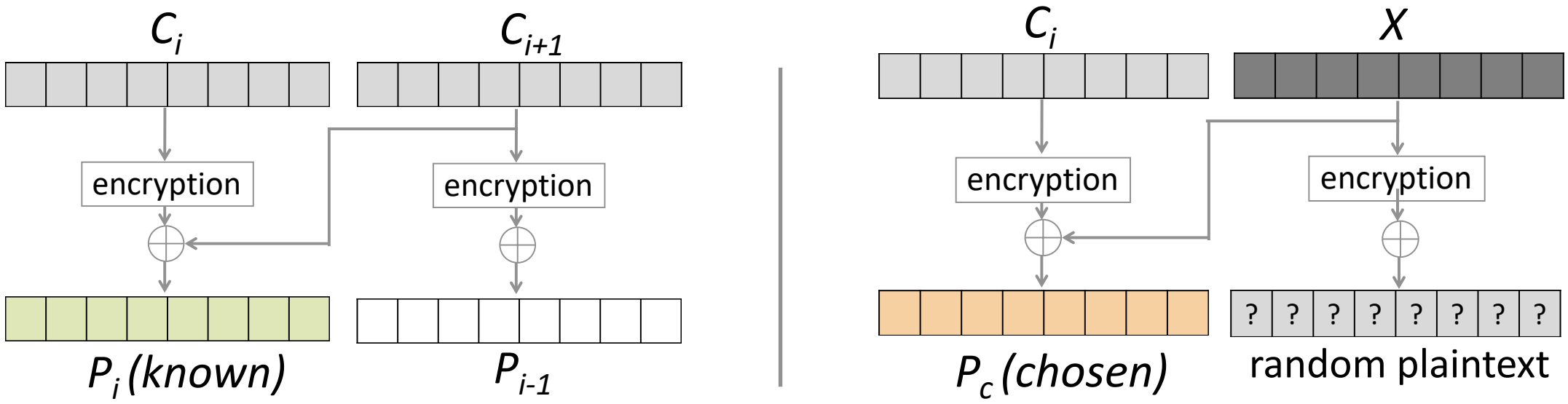
OpenPGP

Attacking OpenPGP

DIFFERENCES TO S/MIME

FH MÜNSTER
University of Applied Sciences

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



Attacking OpenPGP

DEFEATING INTEGRITY PROTECTION

FH MÜNSTER
University of Applied Sciences

Client	Plugin (up to version)	MDC Stripped	MDC Incorrect	SEIP -> SE
Outlook 2007	GPG4WIN 3.0.0			
Outlook 2010	GPG4WIN			
Outlook 2013	GPG4WIN			
Outlook 2016	GPG4WIN			
Thunderbird	Enigmail 1.9.9			
Apple Mail (OSX)	GPGTools 2018.01			

Vulnerable **Not Vulnerable**

Attacking OpenPGP

RFC 4880 ON MODIFICATION DETECTION CODES

FH MÜNSTER
University of Applied Sciences

> 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.

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

FH MÜNSTER
University of Applied Sciences

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

S/MIME

Product	First contact
Outlook 2007	2017-10-25
Outlook 2010	2017-10-25
Outlook 2013	2017-10-25
Outlook 2016	2017-10-25
Win. 10 Mail	2017-10-25
Win. Live Mail	2017-10-25
The Bat!	2018-03-20
Postbox	2018-03-21
eM Client	2018-02-27
IBM Notes	2018-03-20
Thunderbird	2017-10-25
Evolution	2018-02-19
Trojitá	2018-03-10
KMail	2018-02-11
Claws	–
Mutt	–
Apple Mail	2017-11-15
MailMate	2018-02-27
Airmail	2018-03-20
iOS Mail	2017-11-15
R2Mail2	2018-03-10
MailDroid	2018-02-27
Nine	2018-02-27
GMail	2017-11-03
Horde IMP	2018-03-21

Exfiltration channel (no user interaction)
No exfiltration channel found
Exfiltration channel (user interaction required

OpenPGP

Product	First contact
Outlook 2007 / GPG4Win	Out of support
Outlook 2010	–
Outlook 2013	–
Outlook 2016	–
The Bat!	–
Postbox / Enigmail	2018-03-21
eM Client	2018-02-27
Thunderbird / Enigmail	2017-10-25
Evolution	–
Trojitá	–
KMail	–
Claws	–
Mutt	–
Apple Mail / GPGTools	2018-02-16
MailMate	–
Airmail / GPGTools	2018-02-16
Canary Mail	–
K-9 Mail	–
R2Mail2	2018-03-10
MailDroid / Flipdog	2018-02-27
Nine	–
United Internet	–
Mailbox.org	–
ProtonMail	–
Mailfence	–
Roundcube / Enigma	2018-03-28
Horde IMP / GnuPG	2018-03-21
AfterLogic	–
Rainloop	–
Mailpile	–

Exfiltration channel (no user interaction requi
Not vulnerable

Disclosure

Sebastian Schinzel @seecurity · 14. Mai

We'll publish critical vulnerabilities in PGP/GPG and S/MIME email encryption on 2018-05-15 07:00 UTC. They might reveal the plaintext of encrypted emails, including encrypted emails sent in the past. #efail 1/4

Tweet übersetzen

98 2,4 Tsd. 1,9 Tsd.

Sebastian Schinzel @seecurity · 14. Mai

There are currently no reliable fixes for the vulnerability. If you use PGP/GPG or S/MIME for very sensitive communication, you should disable it in your email client for now. Also read @EFF's blog post on this issue: eff.org/deeplinks/2018 … #efail 2/4

Tweet übersetzen

Disclosure

FH MÜNSTER
University of Applied Sciences

Conclusions

FH MÜNSTER
University of Applied Sciences

- 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/