Cryptographic Analysis of Delta Chat

Yuanming Song, Lenka Mareková, Kenneth G. Paterson

Presenter: Matteo Scarlata

ETH zürich

APPLIED CRYPTO GROUP

Delta Chat

- A decentralised messaging application based on e-mail infrastructure.
- Engages with high-risk users (e.g. journalists and activists).

New Study on Multi-tool and Organizational messenger usage

March 31, 2020 by holger

A new Delta Chat UX study is out, based on Xenia's interviews with people engaged in human rights missions in Belarus, Russia, Ukraine, Iran, Taiwan and Hong Kong. It focuses on how Delta Chat could or can already work well in conjunction with other tools and apps, and for organizational settings.

https://delta.chat/en/2020-03-31-needfinding_multidevice

A cryptographic overview

E-mail infrastructure (SMTP, IMAP, …)

A cryptographic overview

(a subset of) **OpenPGP**
E-mail infrastructure (SMTP, IMAP, …)

A cryptographic overview

```
RFC 4880 OpenPGP Message Format
RFC 5581 The Camellia Cipher in OpenPGP
RFC 6637 Elliptic Curve Cryptography (ECC) in OpenPGP
draft-ietf-openpgp-crypto-refresh OpenPGP Message Format
RFC 2015 MIME Security with Pretty Good Privacy (PGP)
RFC 3156 MIME Security with OpenPGP
```

(a subset of) **OpenPGP**
E-mail infrastructure (SMTP, IMAP, …)

A cryptographic overview

“The GnuPG man page is over sixteen thousand words long; for comparison, the novel Fahrenheit 451 is only 40k words.”

Moxie Marlinspike

(a subset of) **OpenPGP**
E-mail infrastructure (SMTP, IMAP, …)

A cryptographic overview

Autocrypt
(a subset of) **OpenPGP**
E-mail infrastructure (SMTP, IMAP, …)

A cryptographic overview

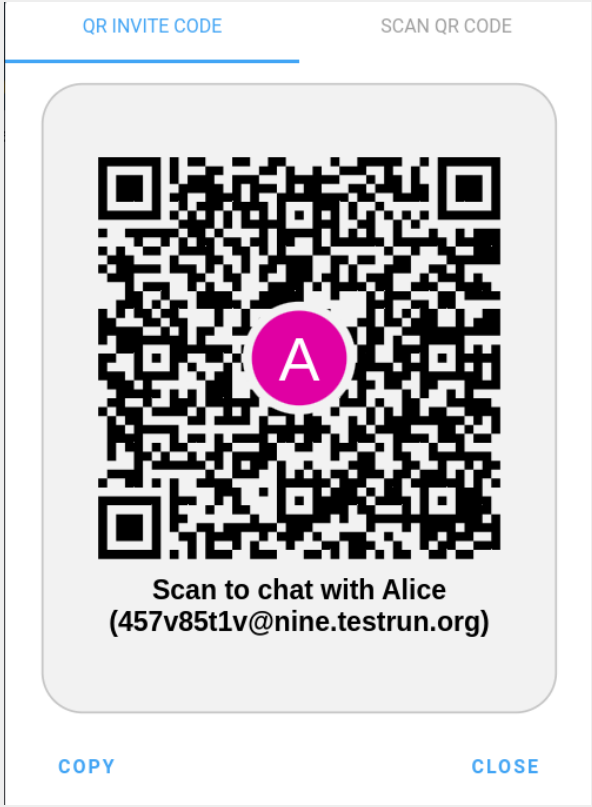
- Automated key management
- TOFU
- “Gossip”: attach keys in email body

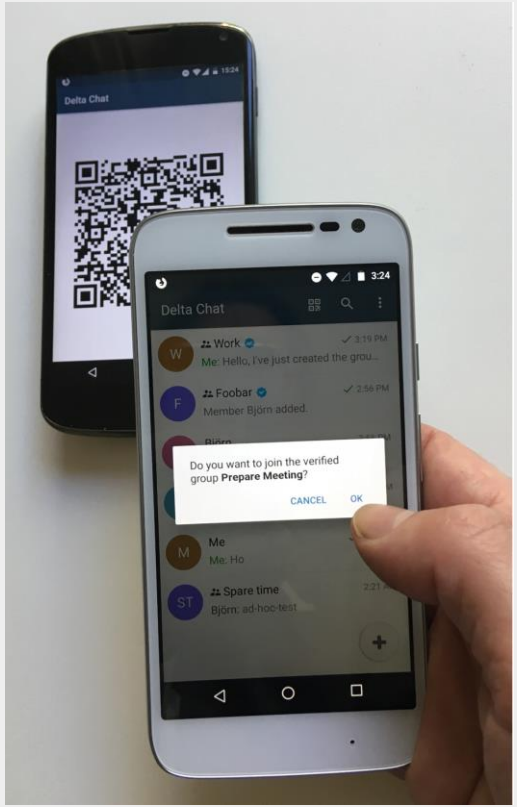
Autocrypt
(a subset of) **OpenPGP**
E-mail infrastructure (SMTP, IMAP, …)

A cryptographic overview

Unverified chats (opportunistic E2EE)	**SecureJoin**
Autocrypt	
(a subset of) **OpenPGP**	
E-mail infrastructure (SMTP, IMAP, …)	

SecureJoin



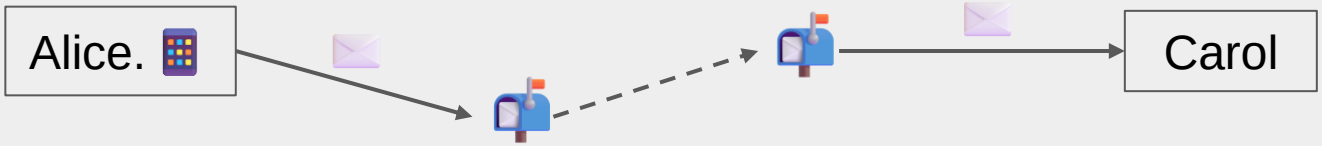


From: Deltachat docs

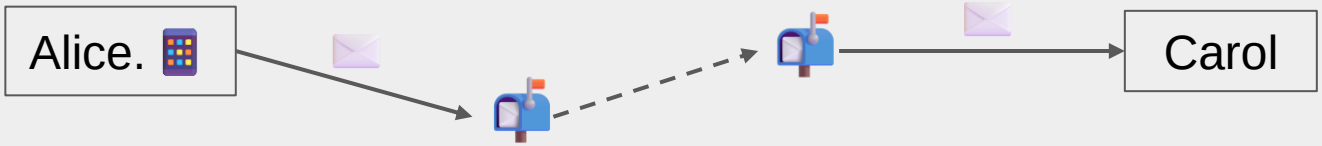
A cryptographic overview

<table>
<tr><td colspan="2">Verified chats (guaranteed E2EE)</td></tr>
<tr><td>Unverified chats
(opportunistic E2EE)</td><td>SecureJoin</td></tr>
<tr><td colspan="2">Autocrypt</td></tr>
<tr><td colspan="2">(a subset of) OpenPGP</td></tr>
<tr><td colspan="2">E-mail infrastructure (TLS, STARTTLS, …)</td></tr>
</table>

Verified chat



Verified chat

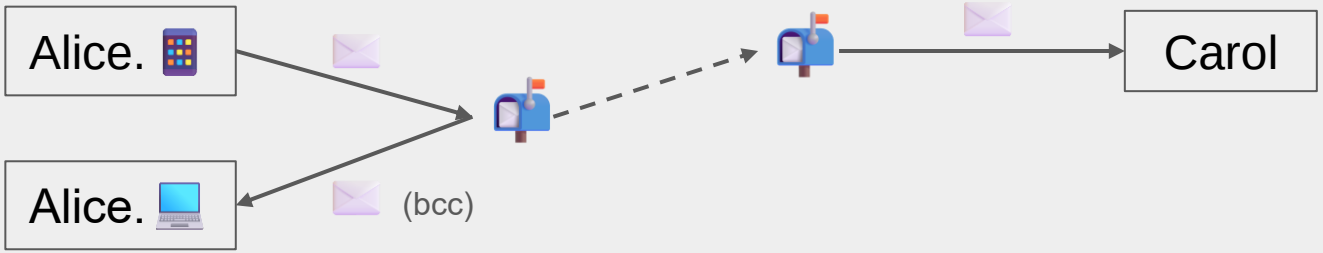



```
From: alice@ethz.ch
To: carol@uzh.ch
Group-ID: M9fXEiVDBYv

Hi Carol! How are you?

[OpenPGP signature]
```

Verified chat




```
From: alice@ethz.ch
To: carol@uzh.ch
Group-ID: M9fXEiVDBYv

Hi Carol! How are you?

[OpenPGP signature]
```

Verified chat

Bob’s verified key: null

Alice. 🏢

📬

📬

Carol

📬

Bob

Verified chat

Bob’s verified key: null

Alice.

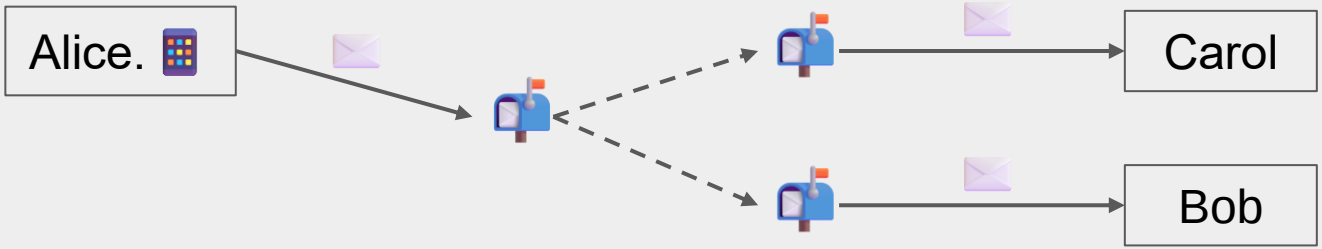
Carol

Bob

```
From: alice@ethz.ch
To: bob@epfl.ch,carol@uzh.ch
Member-Added: bob@epfl.ch
Gossip: (bob@epfl.ch, 🔑)
Group-ID: M9fXEiVDBYv
[...]
[OpenPGP signature]
```

Verified chat

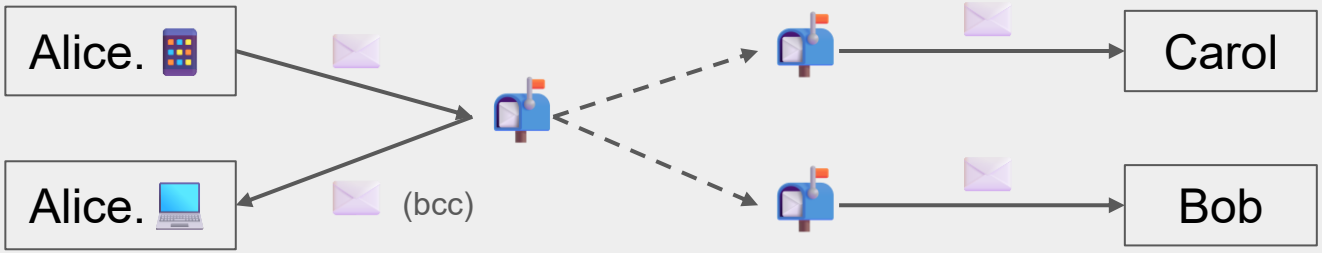
Bob’s verified key: 🔑




```
From: alice@ethz.ch
To: bob@epfl.ch,carol@uzh.ch
Member-Added: bob@epfl.ch
Gossip: (bob@epfl.ch, 🔑)
Group-ID: M9fXEiVDBYv
[...]
[OpenPGP signature]
```

Verified chat

Bob's verified key: 🔑




```
From: alice@ethz.ch
To: bob@epfl.ch,carol@uzh.ch
Member-Added: bob@epfl.ch
Gossip: (bob@epfl.ch, 🔑)
Group-ID: M9fXEiVDBYv
[...]
[OpenPGP signature]
```

Our work

- A deep-dive on the cryptographic algorithms and protocols in Delta Chat, with a view to assessing its security.
- This presentation:
  - **Gossip key injection attack**
  - InsecureJoin observer attack

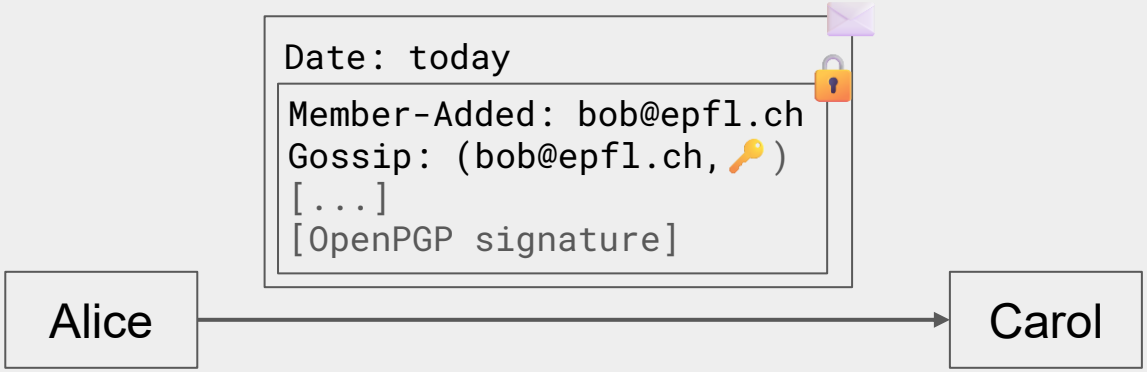
Updating peer states

Alice

Carol

Carol's peers	*gossip_key*	*gossip_time*	*verified_key*	…
Bob	null	null	null	…

Updating peer states



Carol's peers	*gossip_key*	*gossip_time*	*verified_key*	…
Bob	🔑	today	null	…

Updating peer states

```
Date: today
Member-Added: bob@epfl.ch
Gossip: (bob@epfl.ch, 🔑)
[...]
[OpenPGP signature]
```

Alice → Carol

Carol's peers	*gossip_key*	*gossip_time*	*verified_key*	…
Bob	🔑	today	🔑	…

Gossip key injection

Mallory

Carol

Carol's peers	*gossip_key*	*gossip_time*	*verified_key*	…
Bob	null	null	null	…

Gossip key injection

```
Date: Jan 1 2038
Gossip: (bob@epfl.ch, 🔑😈)

Hi Carol!
[OpenPGP signature]
```

Mallory → Carol

Carol's peers	*gossip_key*	*gossip_time*	*verified_key*	…
Bob	🔑😈	Jan 1 2038	null	…

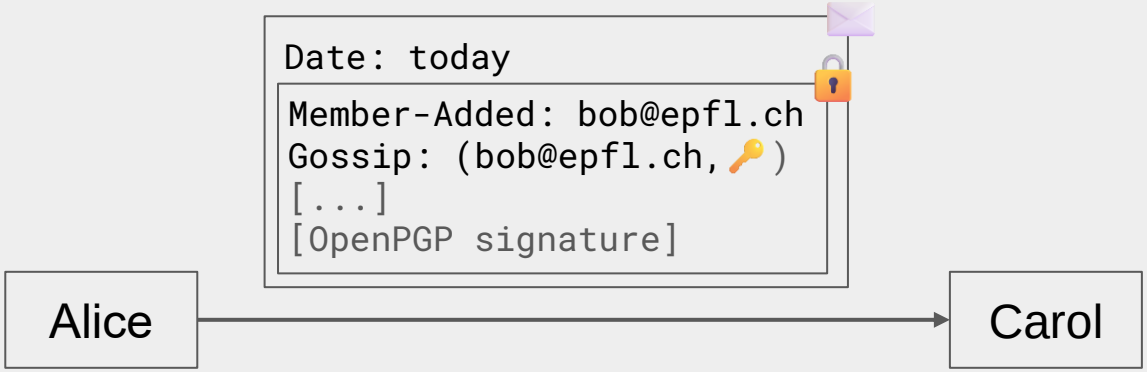
Gossip key injection

```
Date: today
Member-Added: bob@epfl.ch
Gossip: (bob@epfl.ch, 🔑)
[...]
[OpenPGP signature]
```

Alice → Carol

Carol's peers	*gossip_key*	*gossip_time*	*verified_key*	…
Bob	🔑😈	Jan 1 2038	null	…

Gossip key injection



Allows eavesdropping, MITM, impersonation, ...

Carol's peers	*gossip_key*	*gossip_time*	*verified_key*	…
Bob	🔑😈	Jan 1 2038	🔑😈	…

Gossip key injection

Allows eavesdropping, MITM, impersonation, ...

Carol's peers	*gossip_key*	*gossip_time*	*verified_key*	…
Bob		Jan 1 2038		…

Our work

- A deep-dive on the cryptographic algorithms and protocols in Delta Chat, with a view to assessing its security.
- This presentation:
  - Gossip key injection attack
  - **InsecureJoin observer attack**

SecureJoin messages

Alice. 📱

Alice. 💻

📬 📬

Bob

Bob’s verified key: null

SecureJoin messages

Alice. 📱

Alice. 💻

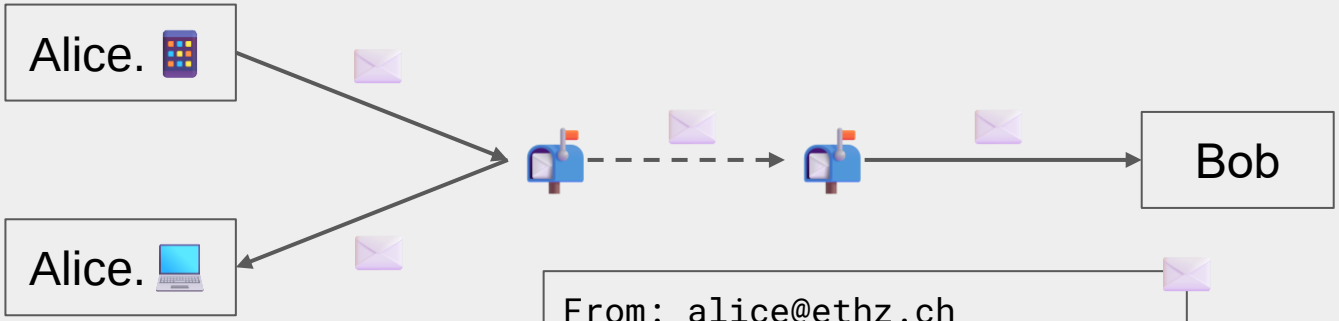
Bob’s verified key: null

Bob

```
From: alice@ethz.ch
To:   bob@epfl.ch
```

```
Secure-Join: contact_confirm
Gossip: (bob@epfl.ch, 🔑)
[...]
[OpenPGP signature]
```

SecureJoin messages



Bob's verified key: 🔑

```
From: alice@ethz.ch
To:   bob@epfl.ch
```

```
Secure-Join: contact_confirm
Gossip: (bob@epfl.ch, 🔑)
[...]
[OpenPGP signature]
```

InsecureJoin observer

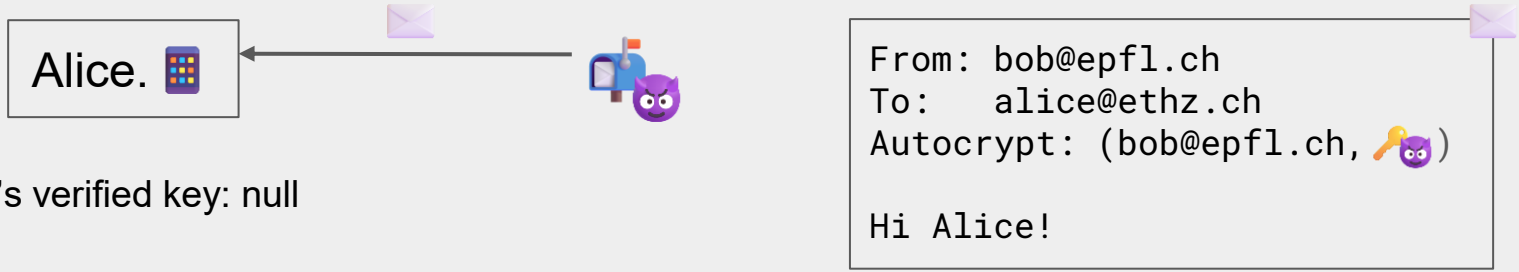
- Confusion between unprotected e-mail headers and protected MIME headers.

Alice. 📱

Bob’s verified key: null

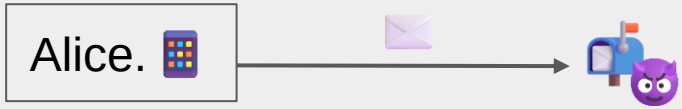
InsecureJoin observer

- Confusion between unprotected e-mail headers and protected MIME headers.



InsecureJoin observer

- Confusion between unprotected e-mail headers and protected MIME headers.



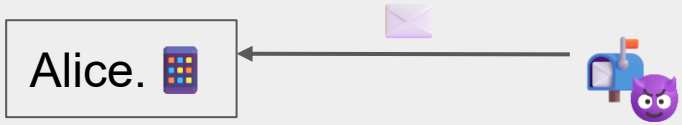
Bob’s verified key: null

```
From:  alice@ethz.ch
To:    bob@epfl.ch

Gossip: (bob@epfl.ch, )
[...]
[OpenPGP signature]
```

InsecureJoin observer

- Confusion between unprotected e-mail headers and protected MIME headers.

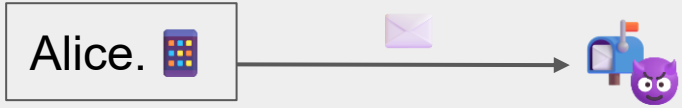


Bob's verified key:

```
From:  alice@ethz.ch
To:    bob@epfl.ch
Secure-Join: contact_confirm
Gossip: (bob@epfl.ch, )
[...]
[OpenPGP signature]
```

InsecureJoin observer

- Confusion between unprotected e-mail headers and protected MIME headers.



Bob's verified key:

```
From: alice@ethz.ch
To:   bob@epfl.ch
```

```
The password is [...]
[OpenPGP signature]
```

Other attacks

Other attacks

- Group member removal – remove members by manipulating e-mail headers.

Other attacks

- Group member removal – remove members by manipulating e-mail headers.
- Synchronisation forgery – forge multi-device synchronisation messages.

Other attacks

- Group member removal – remove members by manipulating e-mail headers.
- Synchronisation forgery – forge multi-device synchronisation messages.
- Autocrypt Setup forgery – forge messages for key transfer between devices.

Other attacks

- Group member removal – remove members by manipulating e-mail headers.
- Synchronisation forgery – forge multi-device synchronisation messages.
- Autocrypt Setup forgery – forge messages for key transfer between devices.
- A compression quine denial-of-service attack.

Other attacks

- Group member removal – remove members by manipulating e-mail headers.
- Synchronisation forgery – forge multi-device synchronisation messages.
- Autocrypt Setup forgery – forge messages for key transfer between devices.
- A compression quine denial-of-service attack.
- Several attacks out of Delta Chat's threat model (e.g. insider attacks).

Disclosure

Coordinated disclosure; all main attacks and most issues have been fixed.

Hardening Guaranteed End-to-End encryption based on a security analysis from ETH researchers

March 25, 2024 by holga, link2xt

We released guaranteed end-to-end encryption in November 2023 and were in for a pleasant surprise three months later. The Applied Cryptography Group at ETH Zurich handed us a cryptographic security analysis of our SecureJoin protocol implementation which is the basis of Delta Chat's guaranteed end-to-end encryption mechanisms. We subsequently fixed 20 identified issues that became part of the v1.44 release but only disclose it now because we first wanted Delta Chat apps with all fixes to be available on all stores.

We'd like to thank the ETH researchers Yuanming Song, Lenka Mareková and Kenneth G. Paterson for their thorough work and their forthcoming communication to resolve questions and review patches. What follows is a timeline and some brief technical discussions of our hardening efforts in response to the cryptographic analysis about which the researchers published separately and in more detail.

https://delta.chat/en/2024-03-25-crypto-analysis-securejoin

Full version at
https://ia.cr/2024/918

- Security analysis
  - Vulnerabilities found even though Deltachat passed several security audits.
  - Root causes: unclear specifications and cross-procol interactions.

- OpenPGP and Autocrypt
  - Careful with non-standard usage and message/key validation.
  - Can benefit from updates, e.g. crypto-refresh for OpenPGP.

Thank you! Questions?