Puncturable Key Wrapping and Its Applications

Matilda Backendal

together with F. Günther and K. Paterson

Applied Cryptography Group
Department of Computer Science
ETH Zurich

December 7, 2022 at ASIACRYPT 2022
Puncturable Key Wrapping
Puncturable Key Wrapping
Puncturable Key Wrapping
Puncturable Key Wrapping

- Encryption of keys
Puncturable Key Wrapping

- Encryption of keys
- Storage/transport
Puncturable Key Wrapping

- Encryption of keys
- Storage/transport
- Key hierarchies
Key Hierarchies

File Encryption
Key Hierarchies

File Encryption
Key Hierarchies

File Encryption
Key Hierarchies

File Encryption

Data Encryption Keys (DEKs)

Files

Outsourced storage
Key Hierarchies

File Encryption

Key Encryption Key (KEK)

Data Encryption Keys (DEKs)

Files

Outsourced storage
Key Hierarchies

File Encryption

Key Encryption Key (KEK)

Wrap

Data Encryption Keys (DEKs)

Files

Outsourced storage
**Key Hierarchies**

**File Encryption**

![Diagram of key hierarchy]

- **Key Encryption Key (KEK)**
- **Wrap**
- **Data Encryption Keys (DEKs)**
- **Files**
- **Outsourced storage**
Key Hierarchies

File Encryption

Key Encryption Key (KEK)

Data Encryption Keys (DEKs)

Files

Wrap

Outsourced storage
Key Hierarchies

File Encryption

Key Encryption Key (KEK)

Wrap

Data Encryption Keys (DEKs)

Files

Outsourced storage
Key Hierarchies

File Encryption

Part of Google’s encryption key hierarchy

Source: https://cloud.google.com/docs/security/encryption/default-encryption
Key Hierarchies

File Encryption

Part of Google’s encryption key hierarchy

Source: https://cloud.google.com/docs/security/encryption/default-encryption
Key Hierarchies

File Encryption

Part of Google’s encryption key hierarchy

Source: https://cloud.google.com/docs/security/encryption/default-encryption
Key Hierarchies

File Encryption

Part of Google’s encryption key hierarchy

Source: https://cloud.google.com/docs/security/encryption/default-encryption
Key Hierarchies

TLS Session Resumption
Key Hierarchies

TLS Session Resumption

Pre-shared keys (PSKs)
Key Hierarchies

TLS Session Resumption

Pre-shared keys (PSKs) → Long-term key

- Pre-shared keys (PSKs) are used for initial encryption of data exchanged between entities.
- The long-term key is generated from a pre-shared secret and used for encrypting the initial PSKs.

This diagram illustrates the process of using pre-shared keys for session resumption in TLS, ensuring secure communication even after a session is interrupted.
Key Hierarchies

TLS Session Resumption

Pre-shared keys (PSKs)  Long-term key
Key Hierarchies

TLS Session Resumption

Pre-shared keys (PSKs) ─────────────────── Long-term key

- Server
- Client
- Server
- Client
Key Hierarchies

TLS Session Resumption

Pre-shared keys (PSKs) → Long-term key

- Pre-shared keys (PSKs)
- Long-term key
Key Hierarchies – Key Compromise
Key Hierarchies – Key Compromise

File Encryption

Key Encryption Key (KEK)

Wrap

DEKs

Files

Outsourced storage
Key Hierarchies – Key Compromise

File Encryption

Key Encryption Key (KEK)

Wrap

DEKs

Files

Outsourced storage
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable

Key Encryption Key (KEK)

Wrap

DEKs

Files

Outsourced storage
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic **key rotation**
File Encryption

Key Encryption Key (KEK)

Wrap

DEKs

Files

Outsourced storage

• All files decryptable
• Including deleted files
• Mitigation: periodic key rotation
• Drawbacks: - re-encryption overhead
Key Hierarchies – Key Compromise

File Encryption

Key Encryption Key (KEK)

Wrap

DEKs

Files

Outsourced storage

• All files decryptable
• Including deleted files
• Mitigation: periodic key rotation
• Drawbacks: - re-encryption overhead
  - coarse-grained & delayed
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
- Drawbacks: - re-encryption overhead
  - coarse-grained & delayed

TLS Session Resumption

- Pre-shared keys
- Long-term key

Outsourced storage
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
- Drawbacks: - re-encryption overhead
  - coarse-grained & delayed

TLS Session Resumption

Pre-shared keys

Long-term key

Outsourced storage
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
- Drawbacks:  - re-encryption overhead
  - coarse-grained & delayed

TLS Session Resumption

- PSKs of past sessions compromised
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
- Drawbacks: - re-encryption overhead
  - coarse-grained & delayed

Outsourced storage

TLS Session Resumption

- PSKs of past sessions compromised
- Violates forward security
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
- Drawbacks: - re-encryption overhead
  - coarse-grained & delayed

TLS Session Resumption

- PSKs of past sessions compromised
- Violates forward security
- Key rotation not possible
Key Hierarchies – Key Compromise

File Encryption

- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
- Drawbacks: - re-encryption overhead
  - coarse-grained & delayed

TLS Session Resumption

- PSKs of past sessions compromised
- Violates forward security
- Key rotation not possible
- Tailored solution [AviramGellertJager19]:
  puncture long-term key

Pre-shared keys

Long-term key

Pre-shared keys

Outsourced storage

Key Encryption Key (KEK)

Wrap

DEKs

Files

Outsourced storage
Key Hierarchies – Key Compromise

File Encryption
- All files decryptable
- Including deleted files
- Mitigation: periodic key rotation
- Drawbacks: - re-encryption overhead
  - coarse-grained & delayed

TLS Session Resumption
- PSKs of past sessions compromised
- Violates forward security
- Key rotation not possible
- Tailored solution [AviramGellertJager19]: puncture long-term key
File Encryption

- All files decryptable
- Including deleted
- Mitigation: periodic key rotation
- Drawbacks: - re-encryption overhead
  - coarse-grained & delayed

TLS Session Resumption

- PSKs of past sessions compromised
- Violates forward security
- Key rotation not possible
- Tailored solution [AviramGellertJager19]: puncture long-term key
**Key Hierarchies – Key Compromise**

### File Encryption
- All files decryptable
- Including deleted
- Mitigation: periodic **key rotation**
- Drawbacks:  
  - re-encryption overhead  
  - coarse-grained & delayed

### TLS Session Resumption
- PSKs of past sessions compromised  
- Violates forward security  
- Key rotation **not possible**  
- Tailored solution [AviramGellertJager19]: **puncture long-term key**
### File Encryption

- **Key Encryption Key (KEK)**
- **DEKs**
- **Files**
  - All files decryptable
  - Including deleted
  - Mitigation: periodic key rotation
  - Drawbacks: re-encryption overhead, coarse-grained & delayed
- **Outsourced storage**

### TLS Session Resumption

- **Pre-shared keys**
  - PSKs of past sessions compromised
  - Violates forward security
  - Key rotation not possible
- **Long-term key**
  - Tailored solution [AviramGellertJager19]: puncture long-term key
Common properties:

File Encryption

- Key Encryption Key (KEK)
- DEKs
- Files
  - All files decryptable
  - Including deleted
  - Mitigation: periodic key rotation
  - Drawbacks:
    - re-encryption overhead
    - coarse-grained & delayed

File Encryption

- Pre-shared keys
- Long-term key

- PSKs of past sessions compromised
- Violates forward security
- Key rotation not possible
- Tailored solution [AviramGellertJager19]:
  - puncture long-term key
File Encryption

Key Encryption Key (KEK)

DEKs

Files

- All files decryptable
- Including deleted
- Mitigation: periodic key rotation
- Drawbacks: - re-encryption overhead
- - coarse-grained & delayed

Outsourced storage

Common properties:

- Key hierarchy

TLS Session Resumption

Pre-shared keys

Long-term key

- PSKs of past sessions compromised
- Violates forward security
- Key rotation not possible
- Tailored solution [AviramGellertJager19]:
  - puncture long-term key
Common properties:

- Key hierarchy
- Benefit from forward security
Common properties:

- Key hierarchy
- Benefit from forward security
- Key rotation not ideal
Common properties:

• Key hierarchy
• Benefit from forward security
• Key rotation not ideal
File Encryption

- All files decryptable
- Including deleted
- Mitigation: periodic key rotation
- Drawbacks: re-encryption overhead, coarse-grained & delayed

TLS Session Resumption

- PSKs of past sessions compromised
- Violates forward security
- Key rotation not possible
- Tailored solution [AviramGellertJager19]: puncture long-term key

Common properties:

- Key hierarchy
- Benefit from forward security
- Key rotation not ideal

Puncturing ❤️ key wrapping = true?
Puncturable Key Wrapping

**File Encryption**
- Key Encryption Key (KEK)
  - KEK
  - DEKs
  - Files
  - All files decryptable
  - Including deleted files
  - Mitigation: periodic key rotation
  - Drawbacks: re-encryption overhead
  - coarse-grained & delayed

**TLS Session Resumption**
- Pre-shared keys
- Long-term key
- PSKs of past sessions compromised
- Violates forward security
- Key rotation not possible
- Tailored solution [AviramGellertJager19]: puncture long-term key

**Drawbacks:**
- re-encryption overhead
- coarse-grained & delayed
Puncturable Key Wrapping

- Fine-grained forward security
Puncturable Key Wrapping

- Fine-grained forward security
- No re-wrapping or key rotation
**File Encryption**

- Key Encryption Key (KEK)
- DEKs
- Files
  - All files decryptable
  - Including deleted files
  - Mitigation: periodic key rotation
  - Drawbacks: re-encryption overhead, coarse-grained & delayed

**TLS Session Resumption**

- Pre-shared keys
- Long-term key
  - PSKs of past sessions compromised
  - Violates forward security
  - Key rotation not possible
  - Tailored solution [AviramGellertJager19]: puncture long-term key

**Puncturable Key Wrapping**

- Fine-grained forward security
- No re-wrapping or key rotation
- Generic
Puncturable Key Wrapping

Syntax & Security
Puncturable Key Wrapping

Syntax & Security

Context $H, k$ → Wrapping key → $\text{Wrap}$
Puncturable Key Wrapping

Syntax & Security
Puncturable Key Wrapping

Syntax & Security

\[ H, \quad \text{Wrap} \quad \text{Wrapping key} \quad H \]

\[ H, \quad \text{Unwrap} \quad H \]
Puncturable Key Wrapping

Syntax & Security

\[ T, H, \xrightarrow{\text{Wrap}} T.H \]  
\[ T, H, \xrightarrow{\text{Unwrap}} \]

Wrapping key

Context

Puncturing tag
Puncturable Key Wrapping

Syntax & Security

Puncturing tag

Context

Wrapping key

Wrap

Unwrap

T, H,

T, H,

T, H,

T
Puncturable Key Wrapping

Syntax & Security

Wrap

Wrap

Unwrap

Punc

T, H, T, H

T

{\(T\)}
Puncturable Key Wrapping

Syntax & Security

Wrap

Unwrap

Puncturing tag

Wrapping key

Context
Puncturable Key Wrapping

Syntax & Security

- **Puncturing tag**: $T, H,$
- **Context**: Wrapping key
- **Unwrap**: $T, H,$
- **Wrap**: $T, H,$
- **Wrapping key**
- **Unwrap**: $T, H,$
- **Punc**: $T$
- **Unwrap**: $\{T\}$
Puncturable Key Wrapping

Syntax & Security

Wrap

Unwrap

Puncturing tag

Wrapping key

Context

Wrap $T, H, \rightarrow \text{Wrap} \rightarrow T, H$

Unwrap $T, H, \rightarrow \text{Unwrap} \rightarrow$

Punc $T \rightarrow \text{Punc} \rightarrow \{T\}$

Unwrap $T, H, \rightarrow \text{Unwrap} \rightarrow \text{Fail}$
Puncturable Key Wrapping

Syntax & Security

Confidentiality: ind$
Puncturable Key Wrapping

Syntax & Security

- **Wrapping key**
- **Confidentiality:** ind$ $T, H$
- **Integrity:** $T, H$

**Puncturing tag**

**Wrap**

$T, H,$

**Context**

**Unwrap**

$T, H,$

Confidentiality: $T, H$

Integrity: $T, H$

Fail

if not honest

**Punc**

$T$

**Unwrap**

$T, H,$

Confidentiality: $T, H$

Integrity: $T, H$

Fail

if not honest

$T$

Fail
Puncturable Key Wrapping

Syntax & Security

Confidentiality: $\text{ind}$

Forward security:

Integrity: $\text{Fail}$ if not honest

Wrapping key

Puncturing tag

Context

Wrap

Unwrap

Punc

T, H, $T, H$

T, H, $T, H$

T

$\{T\}$
Puncturable Key Wrapping

Syntax & Security

Confidentiality: \( \text{ind} \)$

Forward security:

Integrity:

See paper for different flavours of security
Puncturable Key Wrapping

Instantiation
Puncturable Key Wrapping

Instantiation

Wrap
Puncturable Key Wrapping

Instantiation

![Diagram](image-url)
Puncturable Key Wrapping

Instantiation

Wrapping key = PRF key
Puncturable Key Wrapping

Instantiation

Wrap

Puncturing tag = PRF label

Wrapping key = PRF key

T

PRF
Puncturable Key Wrapping

Instantiation

Puncturing tag = PRF label

Wrapping key = PRF key

Wrap

PRF

$T$
Puncturable Key Wrapping

Instantiation

Puncturing tag = PRF label

Context = AD

Wrap

Wrap

PRF

AEAD.Enc

$T$

$H,$

Wrapping key = PRF key
Puncturable Key Wrapping

Instantiation

Wrap

Context = AD

Puncturing tag = PRF label

Wrapping key = PRF key

PRF

H,

AEAD.Enc

T

Wrap

T,H
Puncturable Key Wrapping

Instantiation

Wrap

Puncturing tag = PRF label

Context = AD

Wrapping key = PRF key

Unwrap
Puncturable Key Wrapping

Instantiation

- Puncturing tag = PRF label
- Context = AD
- Wrapping key = PRF key

Wrap:
- $H,$
- $T$

Unwrap:
- $T$

PRF

AEAD.Enc

$T,H$
Puncturable Key Wrapping

Instantiation

Wrap

\[ \text{Wrap} : H, \ AD \rightarrow \text{PRF} \rightarrow \text{AEAD.Enc} \rightarrow T, H \]

Unwrap

\[ \text{Unwrap} : H, T \rightarrow \text{PRF} \rightarrow \text{AEAD.Dec} \rightarrow T, H \]

Wrapping key = PRF key

Puncturing tag = PRF label

Context = AD

December 7, 2022
Matilda Backendal: Puncturable Key Wrapping and Its Applications
Puncturable Key Wrapping

Instantiation

Puncturing tag = PRF label

Context = AD

Wrap

PRF

AEAD.Enc

Unwrap

PRF

AEAD.Dec

Wrapping key = PRF key

Punc
Puncturable Key Wrapping

Instantiation

Puncturing tag = PRF label

Wrap

Context = AD

AEAD.Enc

PPRF

Wrapping key = PRF key

Unwrap

PRF

PRF

Puncturing tag = PRF label

T

H,

T, H

H,

T, H

T

Punc
Puncturable Key Wrapping

Instantiation

- Wrapping key = PRF key
- Puncturing tag = PRF label
- Context = AD

Wrap

\[ \text{Wrap} : H, \text{Context} = \text{AD} \rightarrow \text{AEAD.Enc} \]

Unwrap

\[ \text{Unwrap} : H, \text{Context} = \text{AD} \rightarrow \text{AEAD.Dec} \]

Punc

\[ \text{Punc} : T, \text{PRF.Punc} \rightarrow \text{PRF} \]

December 7, 2022

Matilda Backendal: Puncturable Key Wrapping and Its Applications
Puncturable Key Wrapping

Instantiation

Wrap

Puncturing tag = PRF label

Context = AD

Wrapping key = PRF key

Unwrap

PPRF

T

H,

AEAD.Enc

T, H

AEAD.Dec

H,

T, H

PRF

Puncturing tag = PRF label

PPRF.Punc

T

\{ T \}
Puncturable Key Wrapping

Instantiation

Wrap

Context = AD

Wrapping key = PRF key

Puncturing tag = PRF label

Unwrap

{\(T\)}

PPRF

AEAD.Enc

T

T, H

AEAD.Dec

H, T, H

PPRF.Punc

T

PPRF

December 7, 2022 12

Matilda Backendal: Puncturable Key Wrapping and Its Applications
Puncturable Key Wrapping

Instantiation

Wrap:
- Context = AD
- Wrapping key = PRF key
- Puncturing tag = PRF label

Unwrap:
- Context = AD
- Fail

PPRF

H, T

H, T

{\{T\}}

PPRF.Punc

T
Puncturable Key Wrapping

Instantiation

Wrap

Context = AD

Wrapping key = PRF key

Puncturing tag = PRF label

Unwrap

{\( T \)}

Fail

PPRF

\( H, T, H \)

AEAD.Enc

PPRF.Punc

\( T \)

AEAD.Dec

\( H, T, H \)

PPRF

Fail

\( H, \)}
**Puncturable Key Wrapping**

**Instantiation**

Wrap

- Puncturing tag = PRF label
- Context = AD

Wrap

- Wrapping key = PRF key

Unwrap

- Result:

Fail
Puncturable Key Wrapping

Instantiation

Wrap

Wrapping key = PRF key

Puncturing tag = PRF label

Context = AD

Unwrap

Result:

- Efficient construction
Puncturable Key Wrapping

Instantiation

Wrap

Context = AD

Wrapping key = PRF key

Puncturing tag = PRF label

Result:

• Efficient construction
• Confidentiality & integrity from AEAD
Puncturable Key Wrapping

Instantiation

- Wrapping key = PRF key
- Wrapping tag = PRF label
- Context = AD

Wrap:
- $H, T \rightarrow \text{AEAD.Enc}$
- $T, H \rightarrow \text{PRF}$
- $T \rightarrow \text{PRF.Punc}$

Unwrap:
- $H, T \rightarrow \text{AEAD.Dec}$
- $T \rightarrow \text{PRF}$
- $\{T\} \rightarrow \text{Fail}$

Result:
- Efficient construction
- Confidentiality & integrity from AEAD
- Forward security from PPRF
Puncturable Key Wrapping

Application: Cloud Storage
Puncturable Key Wrapping

Application: Cloud Storage

Diagram:
- Wrapping key
- Context
- Puncturing tag
- Wrapped key
- Unwrapped key
- Punctured key
- Wrapped key
- Unwrapped key
- Punctured key
Puncturable Key Wrapping

Application: Cloud Storage

Wrap

Unwrap

Punc

{T}
Puncturable Key Wrapping

Application: Cloud Storage

For file i:

Wrap

Unwrap

Puncturing tag

Wrapping key

Context

T, H

T

\{T\}
Puncturable Key Wrapping

Application: Cloud Storage

- **Wrap**: Wrapping key
  - Context: $T, H$
  - Puncturing tag

- **Unwrap**: $T, H$

- **Punct**: $T$
  - Puncturing tag
  - Context: $T$

For file $i$:
- Generate $\{T\}$

Diagram:
- User
- File
- Keys
Puncturable Key Wrapping

Application: Cloud Storage

For file $i$:
- Generate
- Encrypt

$\text{Wrap} \leftarrow T, H,$

$\text{Unwrap} \leftarrow T, H,$

$\text{Puncturing tag} \leftarrow T, H,$

$\text{Context} \leftarrow T, H,$

$\text{Wrap} \rightarrow [T]$
Puncturable Key Wrapping

Application: Cloud Storage

For file $i$:
- Generate
- Encrypt
- Sample $T_i$
Puncturable Key Wrapping

Application: Cloud Storage

- Wrap
- Unwrap
- Punc

For file $i$:
- Generate
- Encrypt
- Sample $T_i$
- Wrap $T_i, H_i$
Puncturable Key Wrapping

Application: Cloud Storage

- **Wrap**
  - Context: $T, H$
  - Wrapping key

- **Unwrap**
  - Context: $T, H$

- **Puncturing**
  - Tag: $T, H$
  - Context: $T, H$

For file $i$:
- Generate
- Encrypt
- Sample $T_i$
- Wrap $T, H_i$
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!

File 1 is deleted.
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!

File 1 is deleted. 
Puncturable Key Wrapping

Application: Cloud Storage

Wrap

I want to delete file 1!

Unwrap

Puncturing tag

File 1 is deleted.

Malicious cloud

T, H

{[T]}

T

T, H

T, H

T, H

T, H

T, H

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T

T
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!

File 1 is deleted. not

Malicious cloud
Compromised cloud

T, H
Wrap

Wrapping key

T, H
Unwrap

Context

Puncturing tag

T, H
Wrap

Puncturing tag

T
Punc

{P}

T, H

T_

H

T
t__

H

\ldots

\ldots

\ldots

\ldots

File 1 is deleted.
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!

File 1 is deleted.

Malicious cloud
Compromised cloud
Backups

T

Unwrap

Wrap

Puncturing tag
Context
Wrapping key

{[T]}

T

Punc
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!

File 1 is deleted.

Malicious cloud
Compromised cloud
Backups
Faulty processes

Puncturing tag

Context

Wrapping key

Wrap

Unwrap

Punct

{ }
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!

File 1 is deleted.

Malicious cloud
Compromised cloud
Backups
Faulty processes
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!

File 1 is deleted. not

Malicious cloud
Compromised cloud
Backups
Faulty processes

Puncturing tag
\( T, H \)

Wrap

Unwrap

Wrapping key

Puncturing tag
\( T, H \)

\( T, H \)

\( T, H \)

\( T \)

\( \{T\} \)
Puncturable Key Wrapping

Application: Cloud Storage

- **Wrap**: Wrapping key 
  - Input: Context, Wrapping key 
  - Output: Encrypted data

- **Unwrap**: Unwrapping key
  - Input: Encrypted data, Unwrapping context
  - Output: Key

- **Punc**: Puncturing tag
  - Input: Key, Context
  - Output: Punctured key

- **I want to delete file 1!**

- **File 1 is deleted.**

**Malicious cloud**
- Compromised cloud
- Backups
- Faulty processes

December 7, 2022
Matilda Backendal: Puncturable Key Wrapping and Its Applications
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!

I want to be sure!

File 1 is deleted.

Malicious cloud
Compromised cloud
Backups
Faulty processes
**Puncturable Key Wrapping**

**Application: Cloud Storage**

- **Wrap**
  - Context: $T, H$
  - Wrapping key
  - Puncturing tag

- **Unwrap**
  - $T, H$

- **Puncture**
  - $T$

- **I want to delete file 1!**
  - **I want to be sure!**

- **File 1 is deleted.**

- **Malicious cloud**
- **Compromised cloud**
- **Backups**
- **Faulty processes**

**December 7, 2022**

Matilda Backendal: Puncturable Key Wrapping and Its Applications
Puncturable Key Wrapping

Application: Cloud Storage

I want to delete file 1!

I want to be sure!

File 1 is deleted.

Malicious cloud
Compromised cloud
Backups
Faulty processes
### Puncturable Key Wrapping

#### Application: Cloud Storage

- **Wrap**
  - **Context** \( T, H \)
  - **Wrapping key** \( T, H \)
  - **Puncturing tag** \( T, H \)

- **Unwrap**
  - **Wrap** \( T, H \)
  - **Context** \( T, H \)
  - **Wrapping key** \( T, H \)

- **Punct**
  - **Wrap** \( T \)
  - **Context** \( T \)
  - **Wrapping key** \( T \)

#### Core Components

- **I want to delete file 1!**
- **I want to be sure!**

#### Scenarios

- **Malicious cloud**
- **Compromised cloud**
- **Backups**
- **Faulty processes**

File 1 is deleted.

*December 7, 2022*

Matilda Backendal: Puncturable Key Wrapping and Its Applications
Puncturable Key Wrapping

Application: Cloud Storage

Puncturing tag

Wrap

Unwrap

Punc

I want to delete file 1!

I want to be sure!

File 1 is deleted.

Malicious cloud
Compromised cloud
Backups
Faulty processes

December 7, 2022
Matilda Backendal: Puncturable Key Wrapping and Its Applications
Puncturable Key Wrapping

Application: Cloud Storage

- **Wrap**
  - Context
  - Wrapping key
  - Puncturing tag
  - $T, H$

- **Unwrap**
  - $T, H$

- **Punc**
  - $T$
  - $\{T\}$

- **I want to delete file 1!**
- **I want to be sure!**

- Malicious cloud
- Compromised cloud
- Backups
- Faulty processes

- File 1 is deleted.

- I want to delete file 1!

December 7, 2022
Matilda Backendal: Puncturable Key Wrapping and Its Applications
Puncturable Key Wrapping

Application: Cloud Storage

Puncturing tag

Wrap

Unwrap

Punc

I want to delete file 1!

File 1 is deleted.

Malicious cloud
Compromised cloud
Backups
Faulty processes

I want to be sure!

{\( T_1 \)}

{\( T \)}

\( T, H, T, H \)

\( T, H, T, H \)

\( T \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)

\( T, H, T, H \)
Puncturable Key Wrapping

Application: Cloud Storage

- Fine-grained forward security ✅

Malicious cloud
Compromised cloud
Backups
Faulty processes

I want to delete file 1!
I want to be sure!

File 1 is deleted.
not

I want to delete file 1!
Puncturable Key Wrapping

Application: Cloud Storage

- Fine-grained forward security
- No key rotation or re-wrapping

File 1 is deleted.
Malicious cloud
Compromised cloud
Backups
Faulty processes

I want to delete file 1!
I want to be sure!
Puncturable Key Wrapping

Application: Cloud Storage

- Fine-grained forward security ✅
- No key rotation or re-wrapping ✅
- Generic solution ✅

File 1 is deleted.
Malicious cloud
Compromised cloud
Backups
Faulty processes

I want to delete file 1!
I want to be sure!
Wrapping Up
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive
Wrapping Up

Puncturable Key Wrapping:
A New Cryptographic Primitive

- Provides abstraction layer
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive

- Provides abstraction layer
- Enables fine-grained forward security
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive

- Provides abstraction layer
- Enables fine-grained forward security
- Supports integration into applications
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive

• Provides abstraction layer
• Enables fine-grained forward security
• Supports integration into applications

In the paper:
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive

- Provides abstraction layer
- Enables fine-grained forward security
- Supports integration into applications

In the paper:

- PPRF notions and relations
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive

• Provides abstraction layer
• Enables fine-grained forward security
• Supports integration into applications

In the paper:

• PPRF notions and relations
• PKW notions and relations
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive

• Provides abstraction layer
• Enables fine-grained forward security
• Supports integration into applications

In the paper:

• PPRF notions and relations
• PKW notions and relations
• Integration into TLS
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive

- Provides abstraction layer
- Enables fine-grained forward security
- Supports integration into applications

In the paper:

- PPRF notions and relations
- PKW notions and relations
- Integration into TLS
- Security proofs and bounds
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive

- Provides abstraction layer
- Enables fine-grained forward security
- Supports integration into applications

In the paper:

- PPRF notions and relations
- PKW notions and relations
- Integration into TLS
- Security proofs and bounds
Wrapping Up

Puncturable Key Wrapping: A New Cryptographic Primitive

• Provides abstraction layer
• Enables fine-grained forward security
• Supports integration into applications

In the paper:

• PPRF notions and relations
• PKW notions and relations
• Integration into TLS
• Security proofs and bounds

Thank you!

Get in touch:

mbackendal@inf.ethz.ch
mbackendal.github.io

ePrint: 2022/1209