RUP

Elena Andreeva  Andrey Bogdanov  Atul Luykx
Bart Mennink  Nicky Mouha  Kan Yasuda

FSE 2014 — RUP session
March 4, 2014
RUP:
How to Securely Release Unverified Plaintext in Authenticated Encryption

Elena Andreeva  Andrey Bogdanov  Atul Luykx
Bart Mennink  Nicky Mouha  Kan Yasuda

FSE 2014 — RUP session
March 4, 2014
Authenticated Decryption

$K \downarrow$

$(C, T) \rightarrow \text{AE}^{-1} \rightarrow \begin{cases} M & \text{if } T \text{ is correct} \\ \bot & \text{if } T \text{ is incorrect} \end{cases}$

What if $M$ gets released before tag verification?
Authenticated Decryption

$K \downarrow$

$(C, T) \rightarrow \text{AE}^{-1} \rightarrow \begin{cases} M & \text{if } T \text{ is correct} \\ \bot & \text{if } T \text{ is incorrect} \end{cases}$

What if $M$ gets released before tag verification?
Scenarios

- Insufficient memory
- Insecure memory
- Real-time requirements
- Efficiency reasons
1. First formal study of RUP

2. Security analysis of existing schemes

3. New solutions
1. First formal study of RUP

2. Security analysis of existing schemes

3. New solutions

Thank you!