Computational analysis of EDHOC Stat-Stat

Baptiste COTTIER

HYPOTHESIS

Notations

- $\Pi = (\mathcal{E}, \mathcal{D})$: One-Time Encryption scheme
- $\Pi' = (\mathcal{E}', \mathcal{D}')$: Authenticated Encryption scheme
- $\mathcal{A}$: Adversary

- $\mathbb{G}$: a cyclic group of order p

- sk_i : symmetric keys (denoted as k_i in the specification)
- x_s: Initiator long-term key (denoted as I in the specification)

Diffie-Hellman

- Computational Diffie-Hellman (CDH):
  - Given $(g^u, g^v) \in \mathbb{G}, (u, v) \xleftarrow{\$} \mathbb{Z}_p$, compute g^{uv}
  - Notation: $Adv_{\mathbb{G}}^{CDH}(t) = \max_{\mathcal{A}}(Adv_{\mathbb{G}}^{CDH}(\mathcal{A}))$

Diffie-Hellman

- Computational Diffie-Hellman (CDH):
  - Given $(g^u, g^v) \in \mathbb{G}, (u, v) \xleftarrow{\$} \mathbb{Z}_p$, compute g^{uv}
  - Notation: $Adv_{\mathbb{G}}^{CDH}(t) = \max_{\mathcal{A}}(Adv_{\mathbb{G}}^{CDH}(\mathcal{A}))$

- Gap Diffie-Hellman (GDH):
  - CDH with access to a Decisional Diffie-Hellman oracle
  - Notation: $Adv_{\mathbb{G}}^{GDH}(t, q_{DDH})$

Diffie-Hellman

- Computational Diffie-Hellman (CDH):
  - Given $(g^u, g^v) \in \mathbb{G}, (u, v) \xleftarrow{\$} \mathbb{Z}_p$, compute g^{uv}
  - Notation: $Adv_{\mathbb{G}}^{CDH}(t) = \max_{\mathcal{A}}(Adv_{\mathbb{G}}^{CDH}(\mathcal{A}))$
- Gap Diffie-Hellman (GDH):
  - CDH with access to a Decisional Diffie-Hellman oracle
  - Notation: $Adv_{\mathbb{G}}^{GDH}(t, q_{DDH})$
- Best attack : Baby-Step Giant-Step, $\mathcal{O}(\sqrt{p})$

Symmetric Encryption – One-Time Pad

- Injectivity: $\forall k \in \mathcal{K}, \mathcal{E}(k, m_1) = \mathcal{E}(k, m_2) \Longrightarrow m_1 = m_2$

Symmetric Encryption – One-Time Pad

- Injectivity: $\forall k \in \mathcal{K}, \mathcal{E}(k, m_1) = \mathcal{E}(k, m_2) \Longrightarrow m_1 = m_2$

- One-Time indistinguishability:
  - $\mathcal{E}(k, m_0)$ and $\mathcal{E}(k, m_1)$ are indistinguishable
  - Notation: $Adv_{\Pi}^{OT-ind}(t)$

Symmetric Encryption – AEAD

- Indistinguishability:
  - Given access to an encryption and decryption oracles $\mathcal{E}$ and $\mathcal{D}$
  - $\mathcal{E}'(k, m_0) \cong \mathcal{E}'(k, m_1)$ for a random $k \in \mathcal{K}$,
  - Notation: $Adv_{\Pi'}^{ind}(t)$

Symmetric Encryption – AEAD

- Indistinguishability:
  - Given access to an encryption and decryption oracles $\mathcal{E}$ and $\mathcal{D}$
  - $\mathcal{E}'(k, m_0) \cong \mathcal{E}'(k, m_1)$ for a random $k \in \mathcal{K}$,
  - Notation: $Adv_{\Pi'}^{ind}(t)$

- Unforgeability:
  - Given access to an encryption and decryption oracles $\mathcal{E}$ and $\mathcal{D}$
  - Generate a valid ciphertext
  - Notation: $Adv_{\Pi'}^{uf-cma}(t)$

RESULTS

Notations

- q_{RO} : global number of queries to the random oracles
- n_{σ} : number of running sessions
- N: number of users
- ℓ_{hash}: hash digest length
- ℓ_{MAC}: MAC digest length

Key Privacy

- **Theorem 1**: under the **Gap Diffie-Hellman problem** in the **Random Oracle model**, and the **injectivity** of $(\mathcal{E}\ ,\mathcal{D})$:

$$\boldsymbol{Adv}_{\boldsymbol{EDHOC}}^{\boldsymbol{kp-ake}}\ (\boldsymbol{t}\ ;\boldsymbol{q}_{\boldsymbol{RO}},\boldsymbol{n}_{\boldsymbol{\sigma}}\ ,\boldsymbol{N}) \leq Adv_{\mathbb{G}}^{GDH}\ (t, n_{\sigma}\cdot\ q_{\mathrm{RO}}) + 2N\cdot Adv_{\mathbb{G}}^{GDH}\ (t, q_{\mathrm{RO}}) + \frac{q_{\mathrm{RO}}^{2}+4}{2^{\ell_{hash}+1}}$$

- Best attack:
  - Baby-step Giant-step and the Birthday Paradox
  - $\mathcal{O}(\sqrt{p}\ + 2^{\ell_{hash}/2})$

Explicit Authentication – Responder

- **Theorem 2**: under the Gap Diffie-Hellman problem in the Random Oracle model, and the injectivity of $\Pi = (\mathcal{E}, \mathcal{D})$:

$$\boldsymbol{Adv^{auth-resp}_{EDHOC}\,(t\,; q_{RO}, n_\sigma\,, N)} \leq Adv^{GDH}_{\mathbb{G}}\,(t, n_\sigma \cdot\, q_{\mathrm{RO}}) + 2N \cdot Adv^{GDH}_{\mathbb{G}}\,(t, q_{\mathrm{RO}}) +$$
$$+\ \frac{q_{\mathrm{RO}}^2+2}{2^{\ell_{hash}+1}} + \frac{1}{2^{\ell_{MAC}}}$$

- Best attack:
  - Guess the tag t_2
  - $\mathcal{O}\left(2^{\ell_{MAC}}\right)$

Explicit Authentication – Initiator

- **Theorem 3**: under the Gap Diffie-Hellman problem in the Random Oracle model, and the injectivity of $\Pi = (\mathcal{E}, \mathcal{D})$.

$$\boldsymbol{Adv_{EDHOC}^{auth-init}(t\,;q_{RO}, n_\sigma, N)} \leq Adv_{\mathbb{G}}^{GDH}(t, n_\sigma \cdot q_{\mathrm{RO}}) + 2N \cdot Adv_{\mathbb{G}}^{GDH}(t, q_{\mathrm{RO}}) + \\ + \frac{q_{\mathrm{RO}}^2 + 4}{2^{\ell_{hash}+1}} + \frac{1}{2^{\ell_{MAC}}}$$

- Best attack:
  - Guess the tag t_3
  - $\mathcal{O}(2^{\ell_{MAC}})$
  - **No security provided by $\boldsymbol{sk_3}$ as any imposter can compute it.**

Identity Protection - Responder

- **Theorem 4**: under the **Gap Diffie-Hellman problem** in the **Random Oracle model**, the **injectivity and the semantic security** of $\Pi = (\mathcal{E}, \mathcal{D})$.

$$\boldsymbol{Adv_{EDHOC}^{IdP-resp}(t\,; q_{RO}, n_\sigma, N)} \leq Adv_{\mathbb{G}}^{GDH}(t, n_\sigma \cdot q_{\mathrm{RO}}) + 2N \cdot Adv_{\mathbb{G}}^{GDH}(t, q_{\mathrm{RO}}) + \\ + \frac{q_{\mathrm{RO}}^2 + 2}{2^{\ell_{hash}+1}} + Adv_{\Pi}^{ind}(t)$$

- Best attack:
  - Baby-step Giant-step and the Birthday Paradox
  - $\mathcal{O}(\sqrt{p} + 2^{\ell_{hash}/2})$

Identity Protection - Initiator

- **Theorem 5**: under the **Gap Diffie-Hellman problem** in the **Random Oracle model**, the **injectivity and the semantic security** of $\Pi' = (\mathcal{E}, \mathcal{D})$.

$$\boldsymbol{Adv_{EDHOC}^{IdP-init}(t\,; q_{RO}, n_\sigma, N)} \leq Adv_{\mathbb{G}}^{GDH}(t, n_\sigma \cdot q_{\mathrm{RO}}) + 2N \cdot Adv_{\mathbb{G}}^{GDH}(t, q_{\mathrm{RO}}) + \\ + \frac{q_{\mathrm{RO}}^2 + 2}{2^{\ell_{hash}+1}} + Adv_{\Pi'}^{ind}(t)$$

- Best attack:
  - Baby-step Giant-step and the Birthday Paradox
  - $\mathcal{O}(\sqrt{p} + 2^{\ell_{hash}/2})$

Summary

- Considering Cipher Suits 0 and 2:

AEAD	Hash	MAC length
AES-CCM-16-64-128	SHA-256 (256 bits digest)	64

  - Key Privacy : $\approx$ 128 bits security
  - Mutual Authentication : $\geq$ 64 bits security each
  - Identity Protection : $\approx$ 128 bits security each

Summary

- Considering Cipher Suits 0 and 2:

AEAD	Hash	MAC length
AES-CCM-16-64-128	SHA-256 (256 bits digest)	64

  - Key Privacy : $\approx$ 128 bits security
  - Mutual Authentication : $\geq$ 64 bits security each
  - Identity Protection : $\approx$ 128 bits security each

- Unuse of the unforgeability of Π'
  - sk_3 is independant of x_s
  - Can be computed by an impostor

IMPROVEMENTS

Improved message_3 - $\ell_{MAC} = 128$

- Problem:
  - sk_3 is independant of x_s
  - Around 128 bits security for the Initiator authentication
  - ➢ AEAD is useless

Improved message_3 - $\ell_{MAC} = 128$

- Problem:
  - sk_3 is independant of x_s
  - Around 128 bits security for the Initiator authentication
  - ➢ AEAD is useless

- Solution: Replace $c_3 = \mathcal{E}'(sk_3, IV_3; ID_I \,||\, t_3 \,||\, EAD_3)$ by $\mathcal{E}(sk_3;\ ID_I \,||\, t_3 || \, EAD_3)$ (no need for AEAD)

Improved message_3 - $\ell_{MAC} = 128$

- Problem:
  - sk_3 is independant of x_s
  - Around 128 bits security for the Initiator authentication
  - ➢ AEAD is useless

- Solution: Replace $c_3 = \mathcal{E}'(sk_3, IV_3; ID_I \mid\mid t_3 \mid\mid EAD_3)$ by $\mathcal{E}(sk_3;\ ID_I \mid\mid t_3 \mid\mid EAD_3)$ (no need for AEAD)

- Impacts:
  - Same security (Key Privacy, Mutual Authentication, Identity Protection)
  - Shorter message : len(CIPHERTEXT_3) = len(PLAINTEXT_3) $\leq 128 \times (\left\lfloor \frac{len(PLAINTEXT)\_3-1}{128} \right\rfloor + 1)$

Number of blocks to encrypt with Π’

Improved message_3 - $\ell_{MAC} = 64$

- Problem:
  - sk_3 is independant of x_s
  - Around 64 bits security for the Initiator authentication
  - ➢ AEAD is useless

Improved message_3 - $\ell_{MAC} = 64$

- Problem:
  - sk_3 is independant of x_s
  - Around 64 bits security for the Initiator authentication
  - ➢ AEAD is useless

- Solution: Replace $c_3 = \mathcal{E}'(sk_3, IV_3; ID_I \,||\, t_3 \,||\, EAD_3)$ by $\mathcal{E}(sk_3;\ ID_I || \ EAD_3)||\ \mathcal{E}'(sk_4, IV_4; t_3)$

Depends of x_s

Improved message_3 - $\ell_{MAC} = 64$

- Problem:
  - sk_3 is independant of x_s
  - Around 64 bits security for the Initiator authentication
  - ➢ AEAD is useless

- Solution: Replace $c_3 = \mathcal{E}'(sk_3, IV_3; ID_I \,||\, t_3 \,||\, EAD_3)$ by $\mathcal{E}(sk_3;\ ID_I || \ EAD_3) || \ \mathcal{E}'(sk_4, IV_4; t_3)$

Depends of x_s

- Impacts:
  - Increased Initiaor Authentication Security (+ around 64 bits thanks to the unforgeability of Π' with sk_4)
  - If len$(ID_I || \ EAD_3) \ mod\ 128 \leq$ 64 bits, longer message_3
  - Otherwise, shorter message_3

Improved message_3 - $\ell_{MAC} = 64$

- **Problem**:
  - sk_3 is independant of x_s
  - Around 64 bits security for the Initiator authentication
  - ➢ AEAD is useless

- **Solution**: Replace $c_3 = \mathcal{E}'(sk_3, IV_3; ID_I \mid\mid t_3 \mid\mid EAD_3)$ by $\mathcal{E}(sk_3;\ ID_I \mid\mid EAD_3) \mid\mid \mathcal{E}'(sk_4, IV_4; t_3)$

Depends of x_s

- **Impacts**:
  - Increased Initiaor Authentication Security (+ around 64 bits thanks to the unforgeability of Π' with sk_4)
  - If len$(ID_I \mid\mid EAD_3)$ $mod\ 128 \leq$ 64 bits, longer message_3
  - Otherwise, shorter message_3

- Similar idea can be used for message_2

Better explicit authentication for the responder

Initiator | Responder

m_1 →

← Y_e, c_2, C_R

c_3 →

$sk_4 \leftarrow$ HKDF-Expand(PRK$_{4e3m}$,8, TH$_4$,ℓ_{key})
$IV_4 \leftarrow$ HKDF–Expand(PRK$_{4e3m}$,9, TH$_4$,ℓ_{IV})
$c_4 \leftarrow$ AEAD$(sk_4, IV_4,$ « »)

← c_4

$sk_4 \leftarrow$ HKDF-Expand(PRK$_{4e3m}$,8, TH$_4$,ℓ_{key})
$IV_4 \leftarrow$ HKDF–Expand(PRK$_{4e3m}$,9, TH$_4$,ℓ_{IV})
If $\mathcal{D}(sk_4, c_4) = \perp$, return $\perp$

Better explicit authentication for the responder

Initiator | Responder

m_1 →

← Y_e, c_2, C_R

c_3 →

← c_4

Depends of y_s

$sk_4 \leftarrow$ HKDF-Expand(PRK$_{4e3m}$,8, TH$_4$,ℓ_{key})
$IV_4 \leftarrow$ HKDF−Expand(PRK$_{4e3m}$,9, TH$_4$,ℓ_{IV})
$c_4 \leftarrow \mathrm{AEAD}(sk_4, IV_4,$ « »$)$

Depends of y_s

If valid, $\mathcal{A}$ broke the unforgeability of Π'

$sk_4 \leftarrow$ HKDF-Expand(PRK$_{4e3m}$,8, TH$_4$,ℓ_{key})
$IV_4 \leftarrow$ HKDF−Expand(PRK$_{4e3m}$,9, TH$_4$,ℓ_{IV})
If $\mathcal{D}(sk_4, c_4) = \perp$, return $\perp$

Better explicit authentication for the responder

Initiator | Responder

$\xrightarrow{m_1}$

$\xleftarrow{Y_e, c_2, C_R}$

$\xrightarrow{c_3}$

$\xleftarrow{c_4}$

Depends of y_s

$sk_4 \leftarrow$ HKDF-Expand(PRK$_{4e3m}$,8, TH$_4$,ℓ_{key})
$IV_4 \leftarrow$ HKDF−Expand(PRK$_{4e3m}$,9, TH$_4$,ℓ_{IV})
$c_4 \leftarrow \mathrm{AEAD}(sk_4, IV_4,$ « »$)$

Depends of y_s

If valid, $\mathcal{A}$ broke the unforgeability of Π'

$sk_4 \leftarrow$ HKDF-Expand(PRK$_{4e3m}$,8, TH$_4$,ℓ_{key})
$IV_4 \leftarrow$ HKDF−Expand(PRK$_{4e3m}$,9, TH$_4$,ℓ_{IV})
If $\mathcal{D}(sk_4, c_4) = \perp$, return $\perp$

- Advantage multiplied by $Adv_{\Pi}^{uf-cma}(t) \approx 2^{-64}$
- Responder authentication security ≈ 128 bits

Improved Key Schedule

Non empty nonce for PRK_{2e}

- Factor n_σ in all theorems $(Adv_{\mathbb{G}}^{GDH}(t, n_\sigma \cdot q_{\mathrm{RO}}))$

Improved Key Schedule

Non empty nonce for PRK_{2e}

- Factor n_σ in all theorems $\left(Adv_{\mathbb{G}}^{GDH}\,(t, n_\sigma \cdot\ q_{\mathbf{RO}})\right)$
- Problem: empty string as input of PRK_{2e}
  - $\mathcal{A}$ may match one query to the random oracle with **any** session.

Improved Key Schedule

Non empty nonce for PRK_{2e}

- Factor n_σ in all theorems $\left(Adv_{\mathbb{G}}^{GDH}(t, n_\sigma \cdot q_{\mathbf{RO}})\right)$
- Problem: empty string as input of PRK_{2e}
  - $\mathcal{A}$ may match one query to the random oracle with **any** session.
- Idea: Use TH_2 instead
  - $\mathcal{A}$ may match **one** query to the random oracle with **a chosen** session.

Improved Key Schedule

Non empty nonce for PRK_{2e}

- Factor n_σ in all theorems $\left(Adv_{\mathbb{G}}^{GDH}\left(t, n_\sigma \cdot q_{\mathrm{RO}}\right)\right)$

- Problem: empty string as input of PRK_{2e}
  - $\mathcal{A}$ may match one query to the random oracle with **any** session.

- Idea: Use TH_2 instead
  - $\mathcal{A}$ may match **one** query to the random oracle with **a chosen** session.

- Impacts:
  - No extra cost
  - Advantage becomes $Adv_{\mathbb{G}}^{GDH}\left(t, q_{\mathrm{RO}}\right)$
  - Security independant of n_σ.

Thanks!