Ring Signatures for Deniable AKEM: Gandalf's Fellowship

Phillip Gajland[1,2,3] & **Jonas Janneck**[2] & **Eike Kiltz**[2]

[1] Max Planck Institute for Security and Privacy

[2] Ruhr University Bochum

[3] IBM Research Europe – Zurich

CRYPTO 2024: 44th Annual International Cryptology Conference, Santa Barbara, USA.

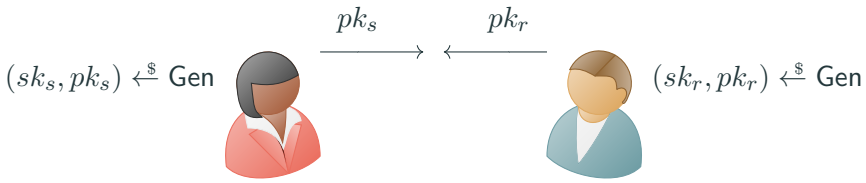
AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]

AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]

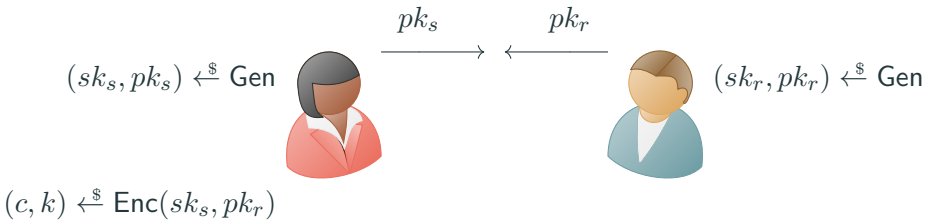
$(sk_s, pk_s) \xleftarrow{\$} \mathsf{Gen}$

$(sk_r, pk_r) \xleftarrow{\$} \mathsf{Gen}$

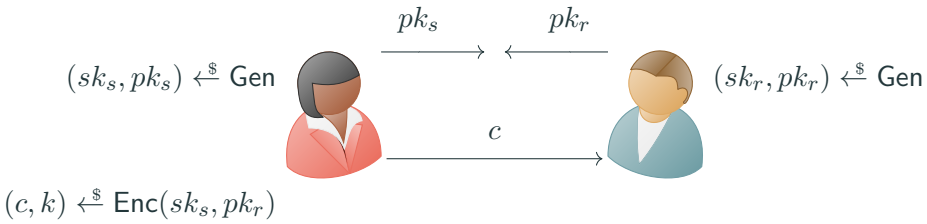
AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]



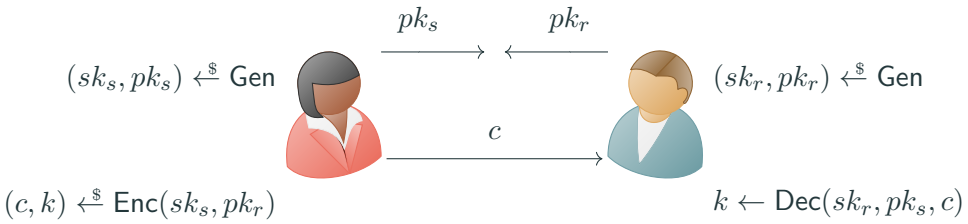
AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]



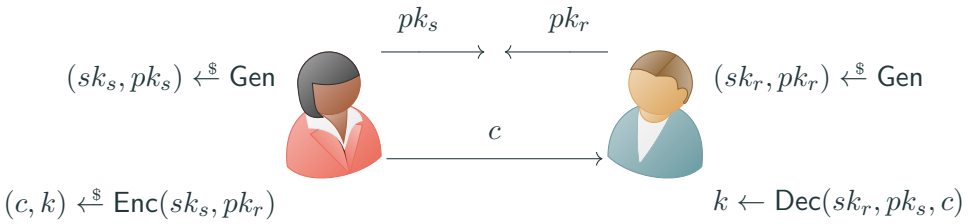
AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]



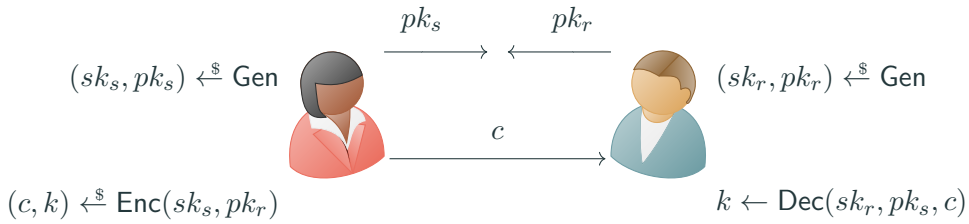
AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]



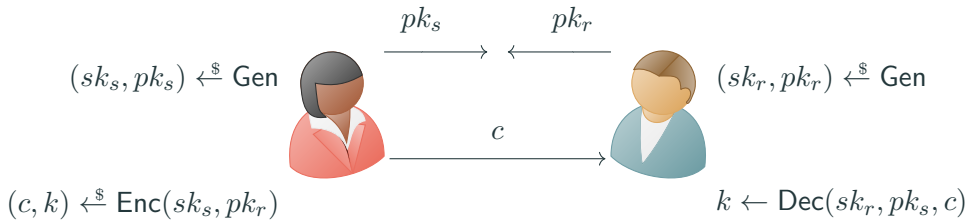
AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]



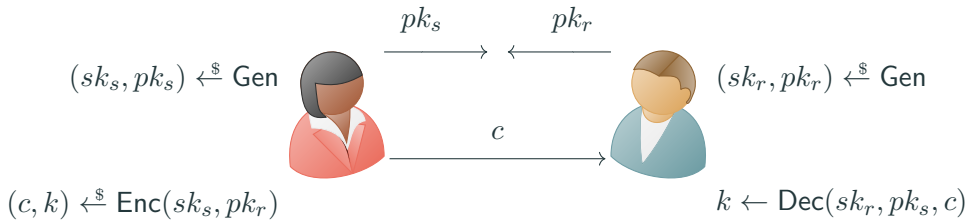
AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]



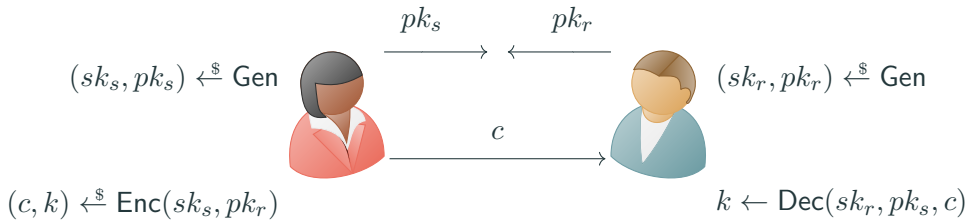
- The primitive behind HPKE [BBLW22] used in MLS [BBR+23]



- The primitive behind HPKE [BBLW22] used in MLS [BBR+23]
- **Confidentiality:** Use CRYSTALS-KYBER [SAB+22]

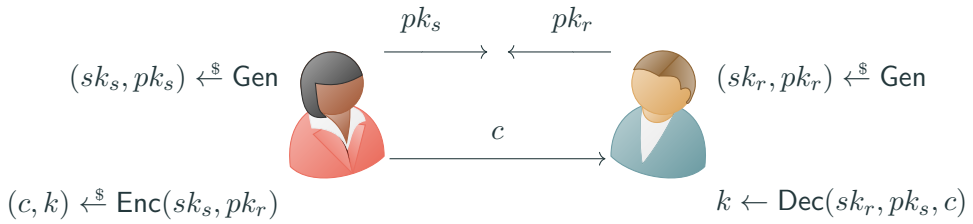


- The primitive behind HPKE [BBLW22] used in MLS [BBR+23]
- **Confidentiality:** Use CRYSTALS-KYBER [SAB+22]
- **Authenticity:** Use CRYSTALS-DILITHIUM [LDK+22]



- The primitive behind HPKE [BBLW22] used in MLS [BBR+23]
- **Confidentiality:** Use CRYSTALS-KYBER [SAB+22]
- **Authenticity:** Use CRYSTALS-DILITHIUM [LDK+22]
- **Deniability:** ✗

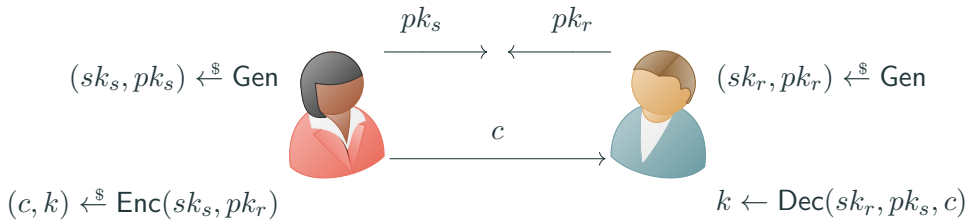
AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]



- The primitive behind HPKE [BBLW22] used in MLS [BBR+23]
- **Confidentiality:** Use CRYSTALS-KYBER [SAB+22]
- **Authenticity:** Use CRYSTALS-DILITHIUM [LDK+22]
- **Deniability:** ✗

} 3.5 KB

AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]



- The primitive behind HPKE [BBLW22] used in MLS [BBR+23]
- **Confidentiality:** Use ~~CRYSTALS-Kyber [SAB+22]~~
- **Authenticity:** Use ~~CRYSTALS-Dilithium [LDK+22]~~

~~3.5 KB~~ 2 KB

- **Deniability:** ~~✗~~ ✓

This work

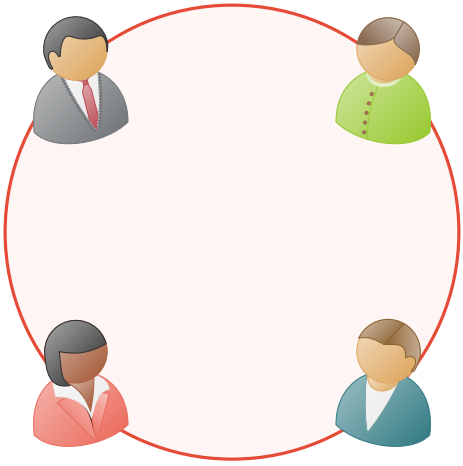
OUTLINE

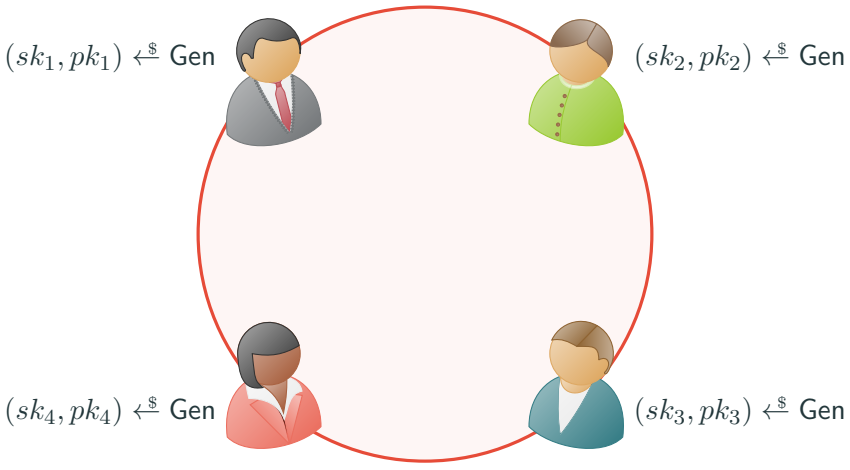
- Ring Signatures
  - Applications and Trade-offs
  - Gandalf Construction and Proof
  - Comparison

- Ring Signatures
  - Applications and Trade-offs
  - GANDALF Construction and Proof
  - Comparison
- Authenticated Key Encapsulation Mechanisms
  - Deniability
  - Black-box Construction and Security
  - Comparison

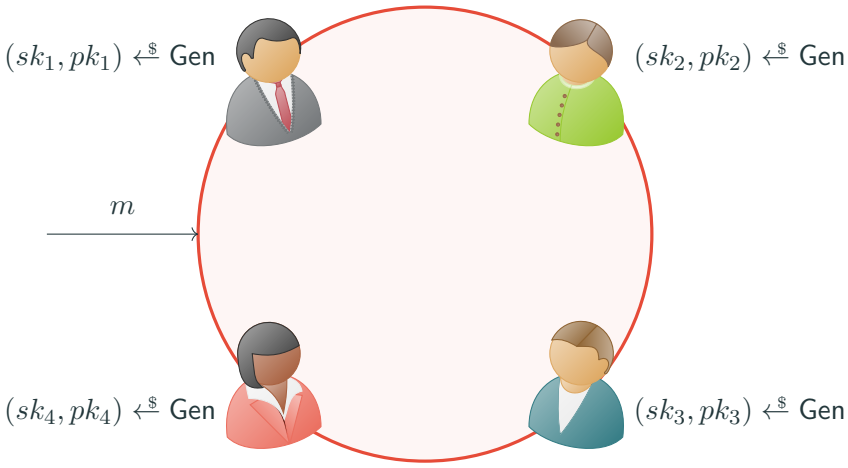
RING SIGNATURES

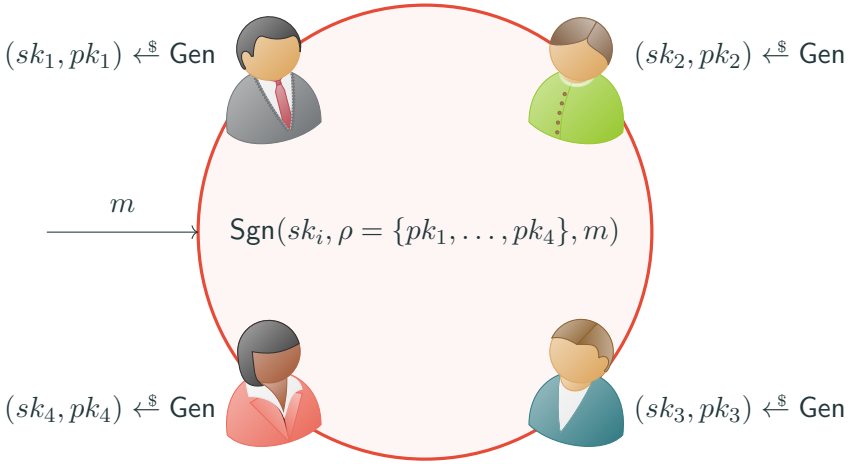
RING SIGNATURE SCHEME (RSig) [RST01]



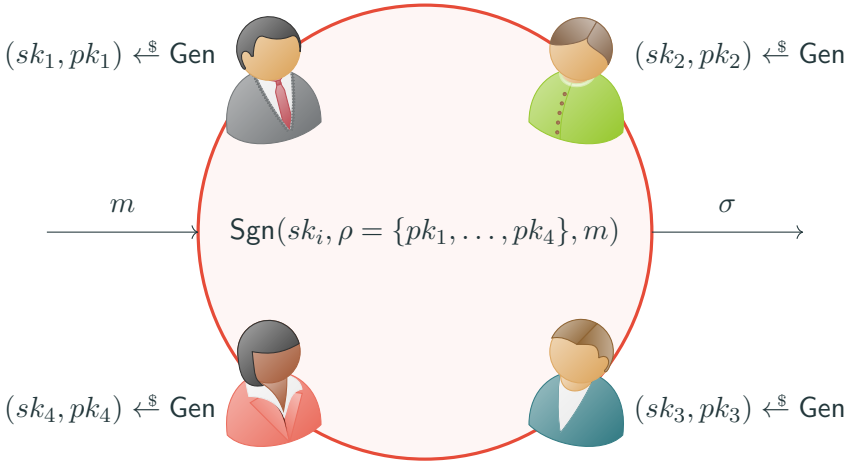

$(sk_1, pk_1) \xleftarrow{\$}$ Gen
$(sk_2, pk_2) \xleftarrow{\$}$ Gen
$(sk_4, pk_4) \xleftarrow{\$}$ Gen
$(sk_3, pk_3) \xleftarrow{\$}$ Gen

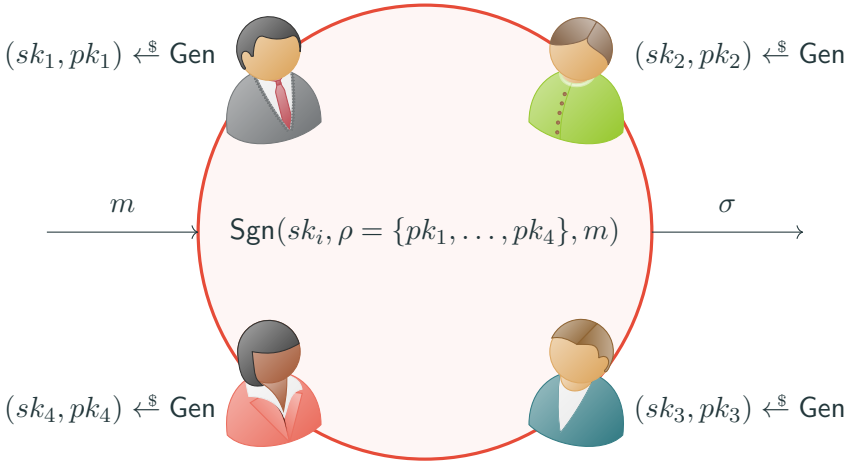
RING SIGNATURE SCHEME (RSig) [RST01]



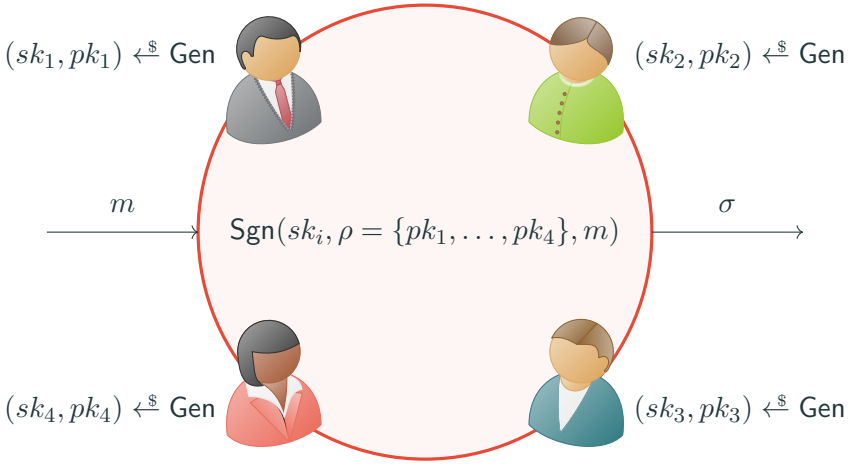

$(sk_1, pk_1) \xleftarrow{\$} \mathsf{Gen}$
$(sk_2, pk_2) \xleftarrow{\$} \mathsf{Gen}$
m
$\mathsf{Sgn}(sk_i, \rho = \{pk_1, \ldots, pk_4\}, m)$
$(sk_4, pk_4) \xleftarrow{\$} \mathsf{Gen}$
$(sk_3, pk_3) \xleftarrow{\$} \mathsf{Gen}$

RING SIGNATURE SCHEME (RSig) [RST01]





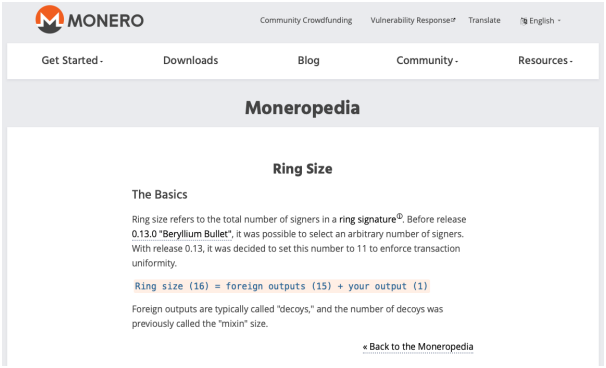
- **Unforgeability:** One sk_i is needed to generate σ .



- **Unforgeability:** One sk_i is needed to generate σ .
- **Anonymity:** Given σ and ρ, it is not possible to identify who signed.

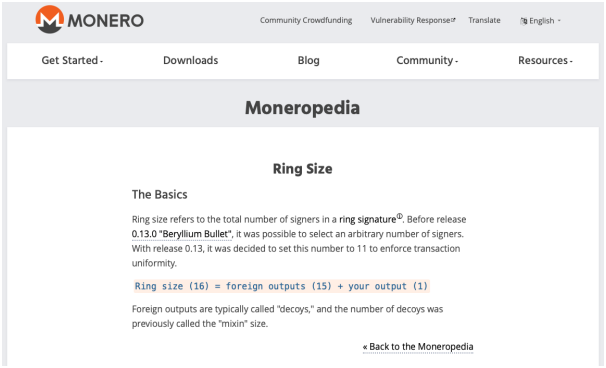
- Originally introduced as a mechanism to protect whistle-blowers.
- Currently used in voting systems and cryptocurrencies such as Dash & Monero.
- Deniable Authentication

RSig SCHEMES ARE DEPLOYED



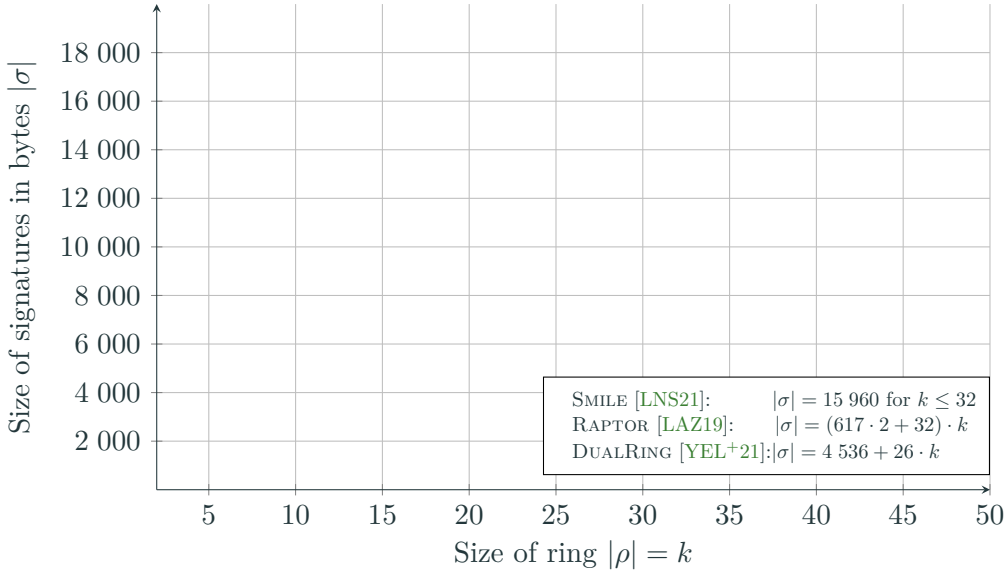
- Originally introduced as a mechanism to protect whistle-blowers.
- Currently used in voting systems and cryptocurrencies such as Dash & Monero.
- Deniable Authentication

RSig SCHEMES ARE DEPLOYED

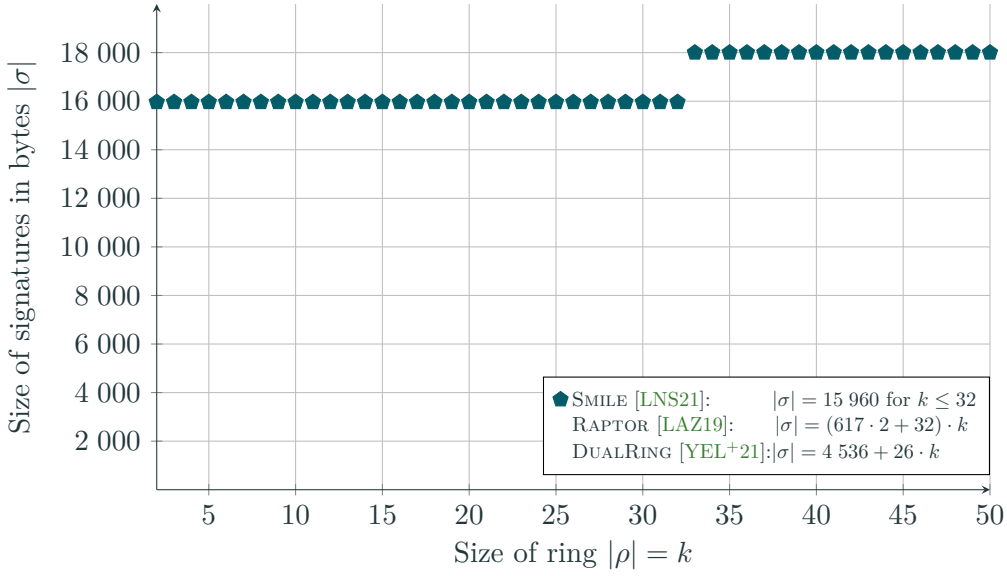


- Originally introduced as a mechanism to protect whistle-blowers.
- Currently used in voting systems and cryptocurrencies such as Dash & Monero.
- Deniable Authentication

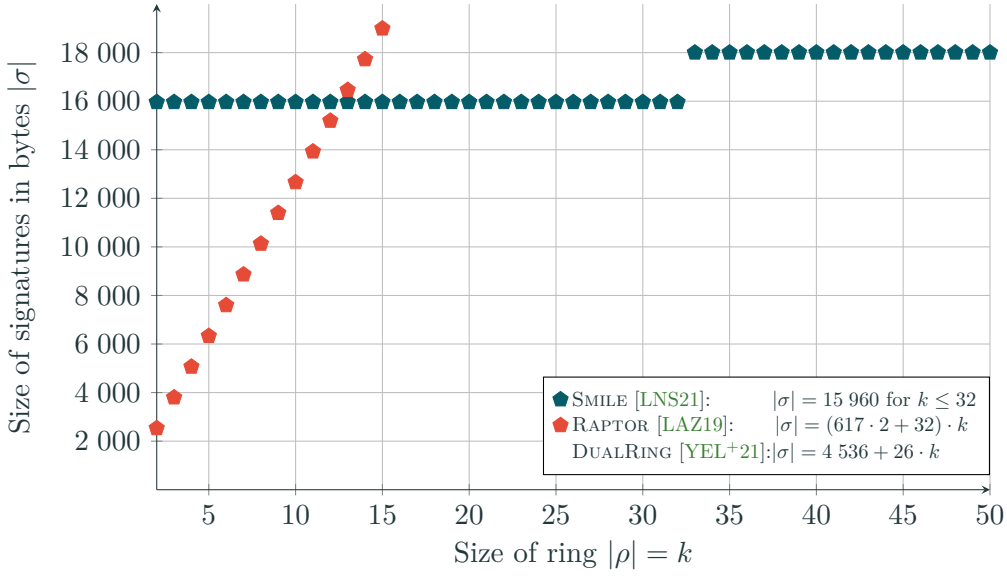
RSig SCHEMES: LINEAR VS SUB-LINEAR



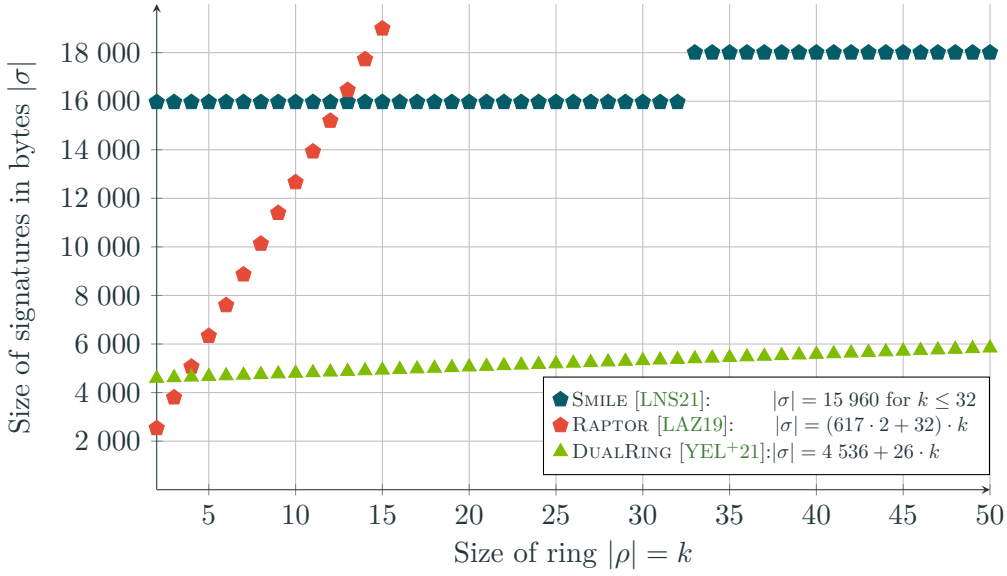
RSig SCHEMES: LINEAR VS SUB-LINEAR



RSig SCHEMES: LINEAR VS SUB-LINEAR



RSig SCHEMES: LINEAR VS SUB-LINEAR



$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

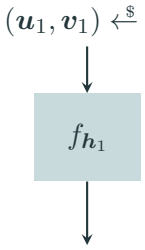
WARMUP: A LINEAR RSig CONSTRUCTION

$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

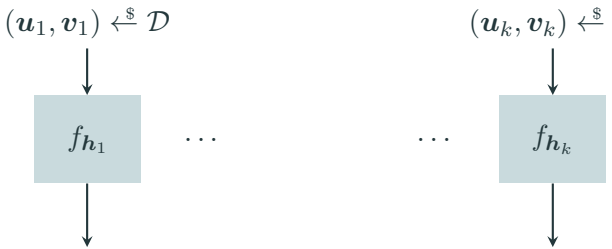
$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$



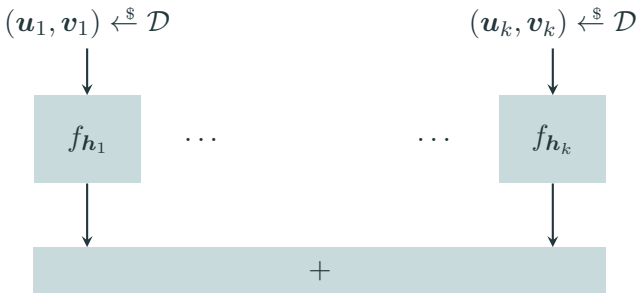
$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$



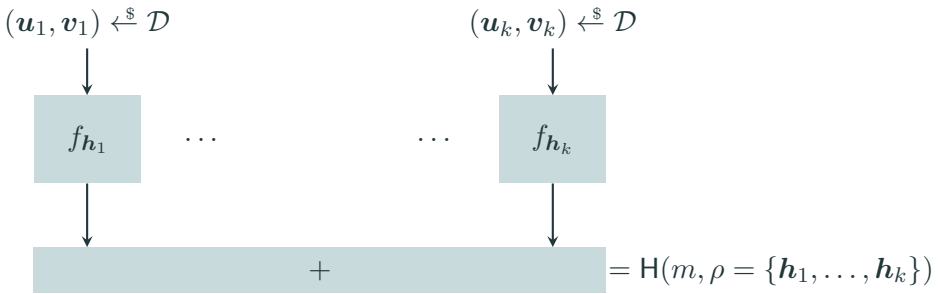
$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$



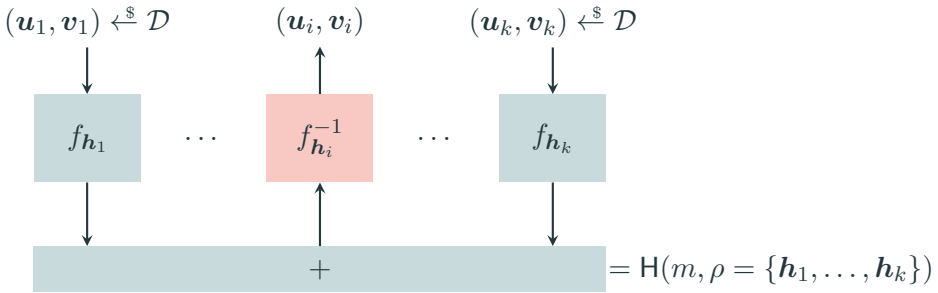
$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$



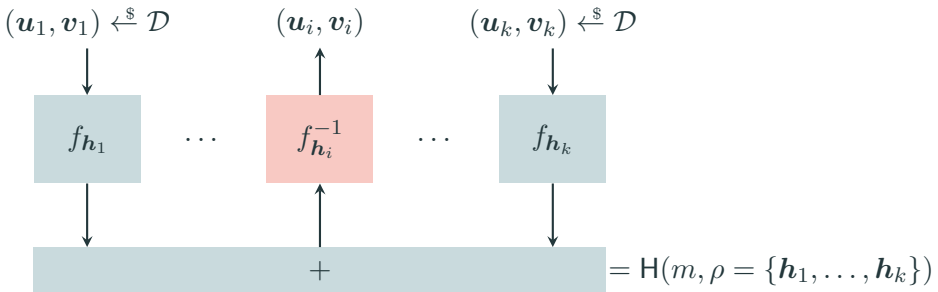
$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$



$$f_{\boldsymbol{h}}\colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1}\colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$



Output $\sigma = (\boldsymbol{u}_1, \boldsymbol{v}_1 \ldots, \boldsymbol{u}_k, \boldsymbol{v}_k)$ such that $\forall\, i \in [k] : \|(\boldsymbol{u}_i, \boldsymbol{v}_i)\|_2 \leq \beta$

$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

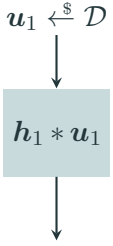
$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

Sgn

$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

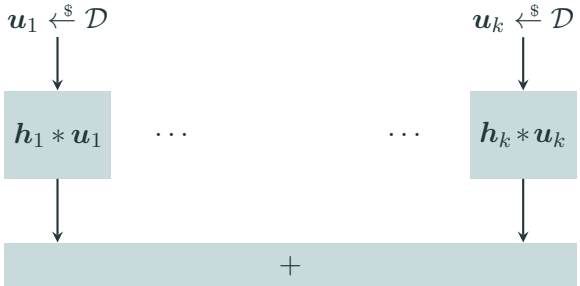
Sgn



$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

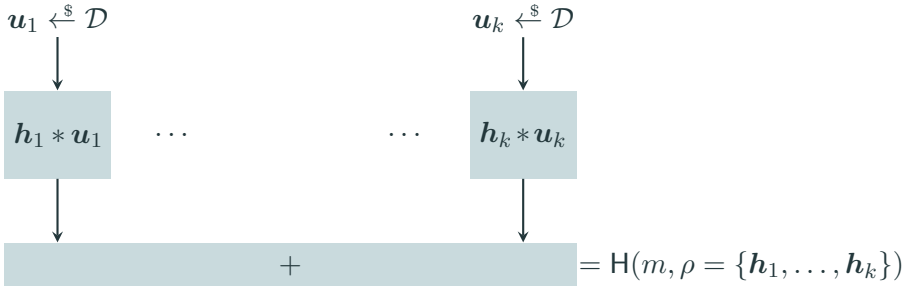
Sgn



$$f_{\boldsymbol{h}}\colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1}\colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

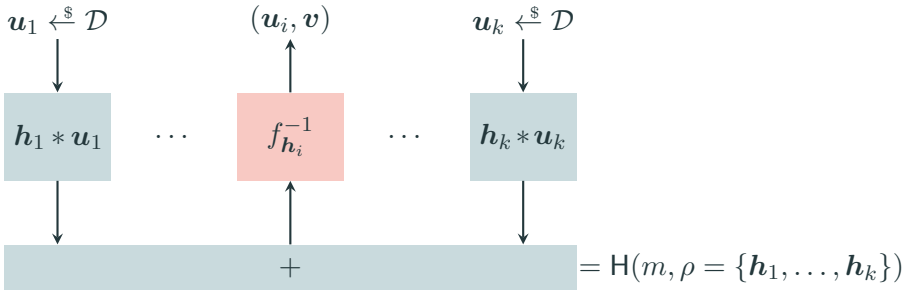
Sgn



$$f_{\boldsymbol{h}}\colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1}\colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

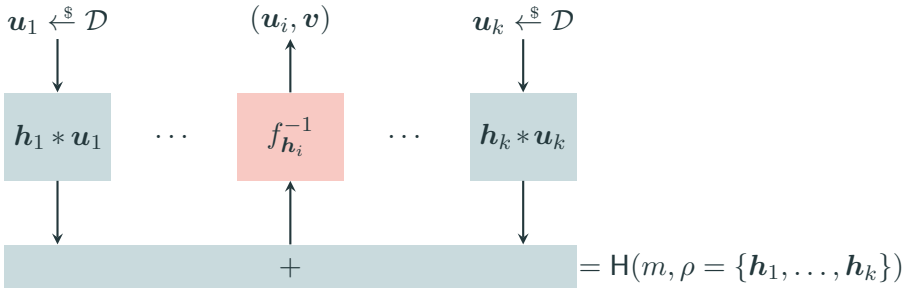
Sgn



$$f_{\boldsymbol{h}}\colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1}\colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

Sgn



Output $\sigma = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) \in \mathcal{R}_q^k$

$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

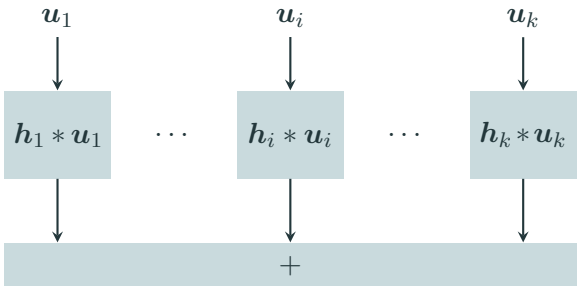
Ver

$\boldsymbol{u}_1$ $\boldsymbol{u}_i$ $\boldsymbol{u}_k$

$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

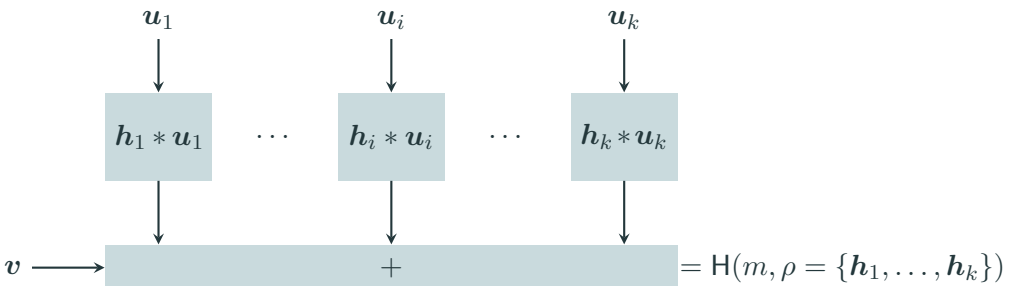
Ver



$$f_{\boldsymbol{h}} \colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

$$f_{\boldsymbol{h}}^{-1} \colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

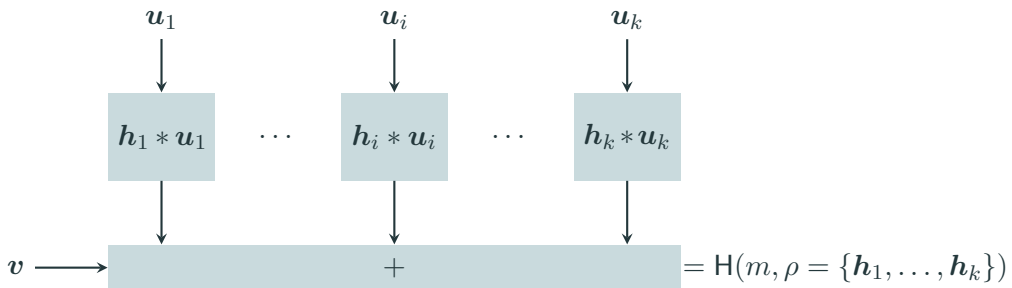
Ver



$$f_{\boldsymbol{h}}\colon \mathcal{R}_q \times \mathcal{R}_q \to \mathcal{R}_q$$
$$(\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{h} * \boldsymbol{u} + \boldsymbol{v}$$

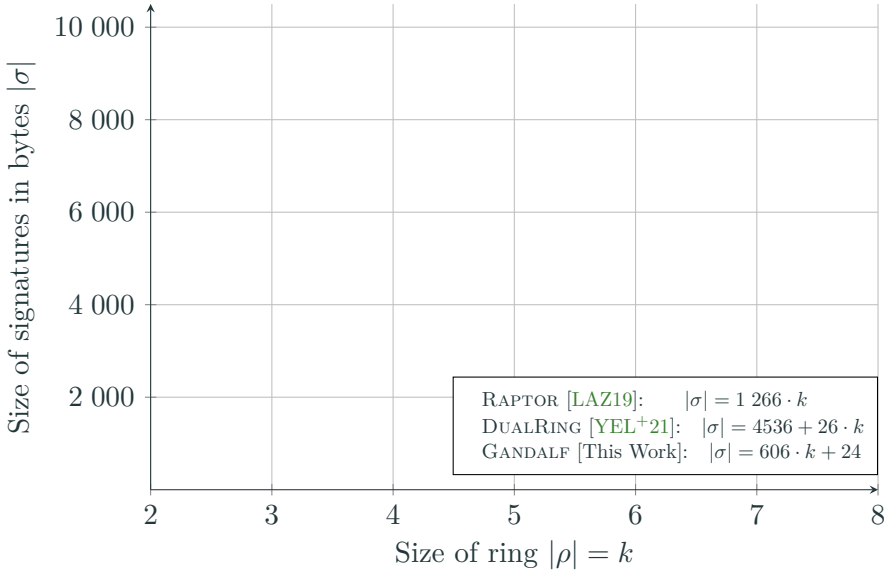
$$f_{\boldsymbol{h}}^{-1}\colon \boldsymbol{c} \mapsto (\boldsymbol{u}, \boldsymbol{v}) \sim \mathcal{D}^2_{|\boldsymbol{h}*\boldsymbol{u}+\boldsymbol{v}=\boldsymbol{c}}$$

Ver

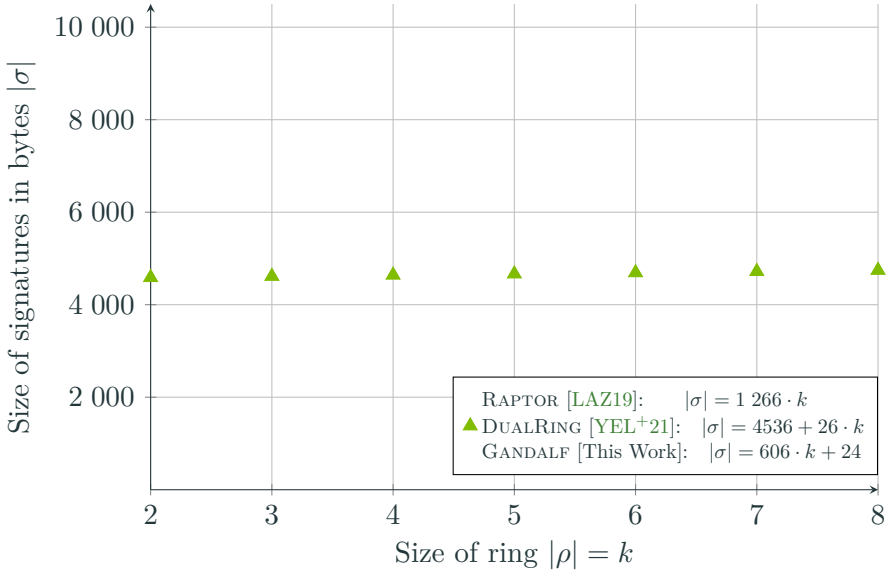


Check that: $\|(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \boldsymbol{v})\|_2 \leq \beta$

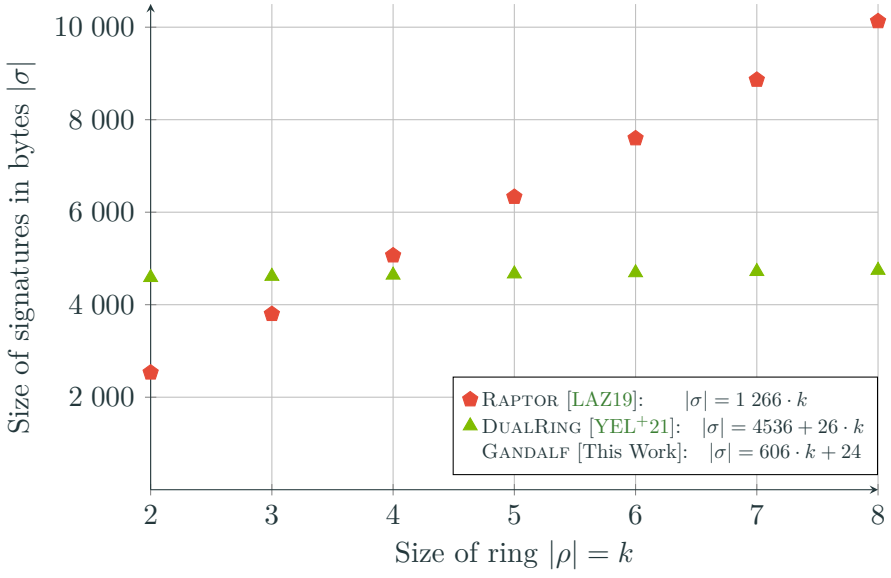
Gandalf: comparison to other linear RSig schemes



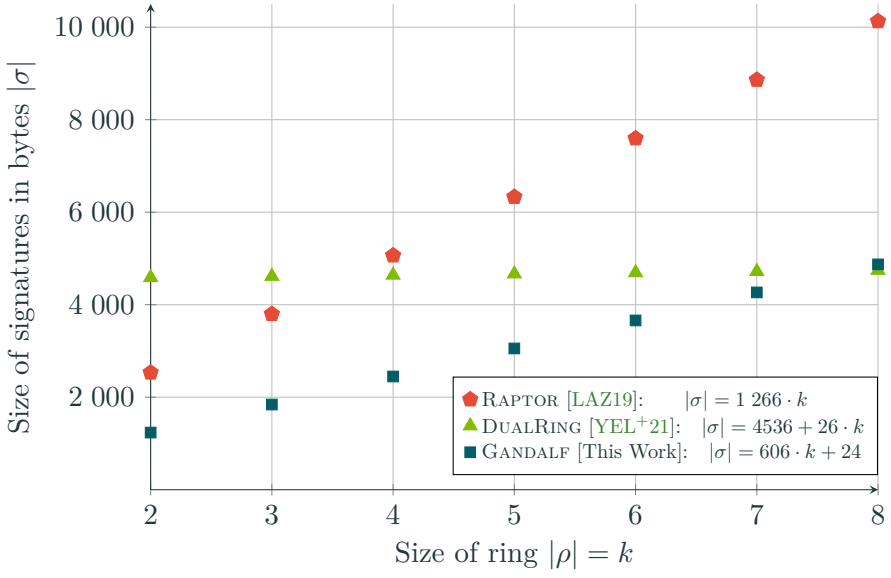
Gandalf: comparison to other linear RSig schemes

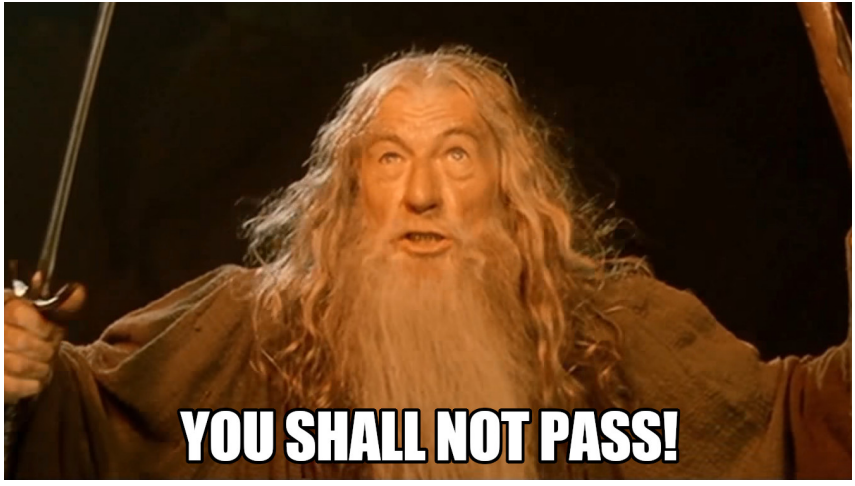


Gandalf: comparison to other linear RSig schemes



Gandalf: comparison to other linear RSig schemes




YOU SHALL NOT PASS!

Gandalf security bounds

- **Unforgeability:** One-per-message unforgeability under chosen ring attacks

- **Unforgeability:** One-per-message unforgeability under chosen ring attacks

$$Adv^{(\mathrm{n},\kappa,Q_{\mathsf{Sgn}})\text{-}\mathbf{UF\text{-}CRA1}}_{\textsc{Gandalf}[\mathsf{TpdGen},\mathsf{PreSmp}]} \leq Q_{\mathsf{H}} \cdot Adv^{\mathcal{R}\text{-}\mathbf{LWE}}_{m=1,q,\alpha,s}$$

- **Unforgeability:** One-per-message unforgeability under chosen ring attacks

$$Adv^{(\mathrm{n},\kappa,Q_{\mathsf{Sgn}})\text{-}\mathbf{UF\text{-}CRA1}}_{\textsc{Gandalf}[\mathsf{TpdGen},\mathsf{PreSmp}]} \leq Q_{\mathsf{H}} \cdot Adv^{\mathcal{R}\text{-}\mathbf{LWE}}_{m=1,q,\alpha,s} + c \cdot Q_{\mathsf{H}} \cdot \mathrm{Adv}^{\mathcal{R}\text{-}\mathbf{ISIS}}_{m=n,q,\alpha,\beta}$$

- **Unforgeability:** One-per-message unforgeability under chosen ring attacks

$$Adv^{(\mathrm{n},\kappa,Q_{\mathsf{Sgn}})\text{-}\mathbf{UF\text{-}CRA1}}_{\textsc{Gandalf}[\mathsf{TpdGen},\mathsf{PreSmp}]} \leq Q_{\mathsf{H}} \cdot Adv^{\mathcal{R}\text{-}\mathbf{LWE}}_{m=1,q,\alpha,s} + c \cdot Q_{\mathsf{H}} \cdot \mathrm{Adv}^{\mathcal{R}\text{-}\mathbf{ISIS}}_{m=n,q,\alpha,\beta}$$

$$\text{for } \beta = \tau s\sqrt{(\kappa+1)N}$$

- **Unforgeability:** One-per-message unforgeability under chosen ring attacks

$$Adv^{(\mathrm{n},\kappa,Q_{\mathsf{Sgn}})\text{-}\mathbf{UF\text{-}CRA1}}_{\textsc{Gandalf}[\mathsf{TpdGen},\mathsf{PreSmp}]} \leq Q_{\mathsf{H}} \cdot Adv^{\mathcal{R}\text{-}\mathbf{LWE}}_{m=1,q,\alpha,s} + c \cdot Q_{\mathsf{H}} \cdot \mathrm{Adv}^{\mathcal{R}\text{-}\mathbf{ISIS}}_{m=n,q,\alpha,\beta}$$

$$\text{for } \beta = \tau s\sqrt{(\kappa+1)N} \text{ and } c = \sqrt{2} \cdot R_{2\lambda}(\mathsf{PreSmp} \mid\mid \mathcal{D})^{Q_{\mathsf{Sgn}}}.$$

- **Unforgeability:** One-per-message unforgeability under chosen ring attacks

$$Adv^{(\mathrm{n},\kappa,Q_{\mathsf{Sgn}})\text{-}\mathbf{UF\text{-}CRA1}}_{\textsc{Gandalf}[\mathsf{TpdGen},\mathsf{PreSmp}]} \leq Q_{\mathsf{H}} \cdot Adv^{\mathcal{R}\text{-}\mathbf{LWE}}_{m=1,q,\alpha,s} + c \cdot Q_{\mathsf{H}} \cdot \mathrm{Adv}^{\mathcal{R}\text{-}\mathbf{ISIS}}_{m=n,q,\alpha,\beta} + \frac{c}{|\mathcal{R}_q|},$$

$$\text{for } \beta = \tau s\sqrt{(\kappa+1)N} \text{ and } c = \sqrt{2} \cdot R_{2\lambda}(\mathsf{PreSmp} \mid\mid \mathcal{D})^{Q_{\mathsf{Sgn}}}.$$

- **Unforgeability:** One-per-message unforgeability under chosen ring attacks

$$Adv^{(\mathrm{n},\kappa,Q_{\mathsf{Sgn}})\text{-}\mathbf{UF\text{-}CRA1}}_{\textsc{Gandalf}[\mathsf{TpdGen},\mathsf{PreSmp}]} \leq Q_{\mathsf{H}} \cdot Adv^{\mathcal{R}\text{-}\mathbf{LWE}}_{m=1,q,\alpha,s} + c \cdot Q_{\mathsf{H}} \cdot \mathrm{Adv}^{\mathcal{R}\text{-}\mathbf{ISIS}}_{m=n,q,\alpha,\beta} + \frac{c}{|\mathcal{R}_q|},$$

$$\text{for } \beta = \tau s\sqrt{(\kappa+1)N} \text{ and } c = \sqrt{2} \cdot R_{2\lambda}(\mathsf{PreSmp} \mid\mid \mathcal{D})^{Q_{\mathsf{Sgn}}}.$$

- **Anonymity:** Under full key exposure and multiple challenges

- **Unforgeability:** One-per-message unforgeability under chosen ring attacks

$$Adv^{(\mathrm{n},\kappa,Q_{\mathtt{Sgn}})\text{-}\mathbf{UF\text{-}CRA1}}_{\textsc{Gandalf}[\mathsf{TpdGen},\mathsf{PreSmp}]} \leq Q_{\mathsf{H}} \cdot Adv^{\mathcal{R}\text{-}\mathbf{LWE}}_{m=1,q,\alpha,s} + c \cdot Q_{\mathsf{H}} \cdot \mathrm{Adv}^{\mathcal{R}\text{-}\mathbf{ISIS}}_{m=n,q,\alpha,\beta} + \frac{c}{|\mathcal{R}_q|},$$

$$\text{for } \beta = \tau s\sqrt{(\kappa+1)N} \text{ and } c = \sqrt{2} \cdot R_{2\lambda}(\mathsf{PreSmp} \mid\mid \mathcal{D})^{Q_{\mathtt{Sgn}}}.$$

- **Anonymity:** Under full key exposure and multiple challenges

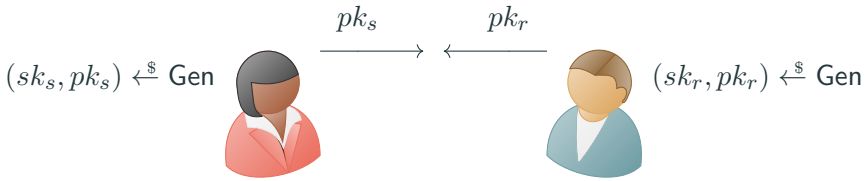
$$\mathrm{Adv}^{(n,Q_{\mathtt{Chl}})\text{-}\mathbf{MC\text{-}Ano}}_{\textsc{Gandalf}[\mathsf{TpdGen},\mathsf{PreSmp}]} \leq Q_{\mathtt{Chl}} \cdot KL(\mathsf{PreSmp} \mid\mid \mathcal{D}).$$

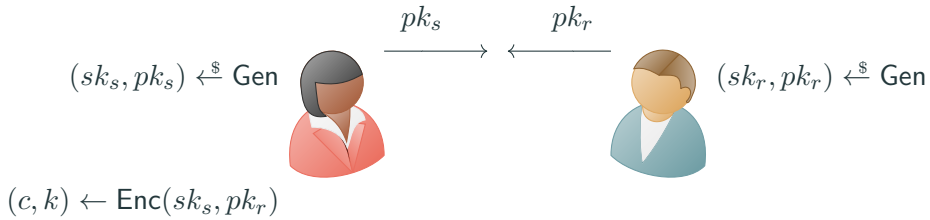
AKEM

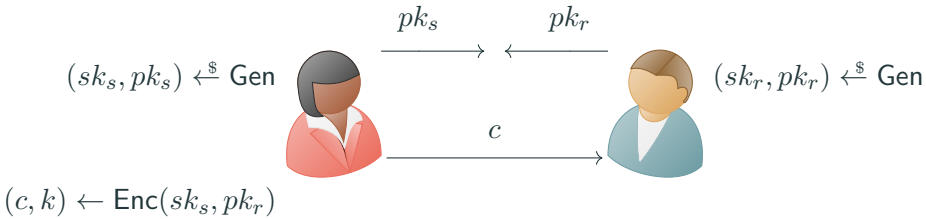
AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]

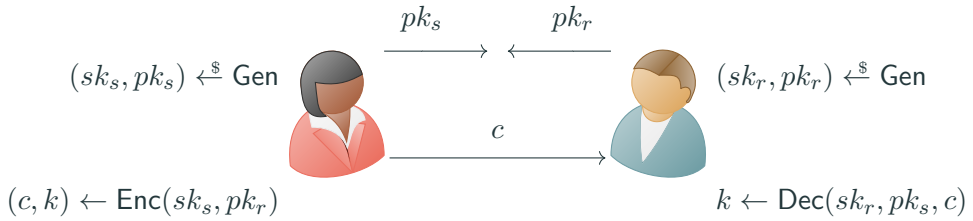
$(sk_s, pk_s) \xleftarrow{\$} \mathsf{Gen}$

$(sk_r, pk_r) \xleftarrow{\$} \mathsf{Gen}$

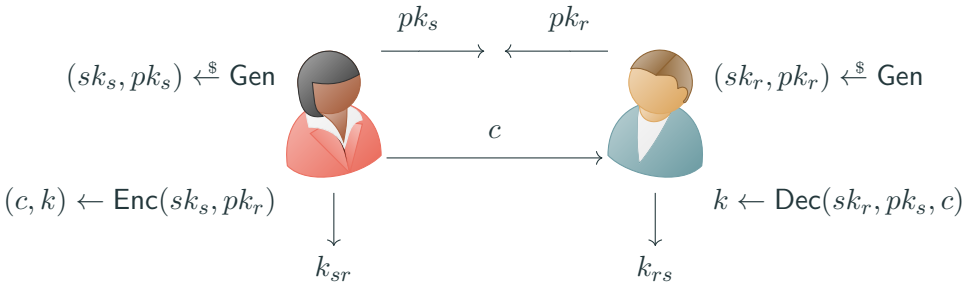

pk_s
pk_r
$(sk_s, pk_s) \xleftarrow{\$} \mathsf{Gen}$
$(sk_r, pk_r) \xleftarrow{\$} \mathsf{Gen}$

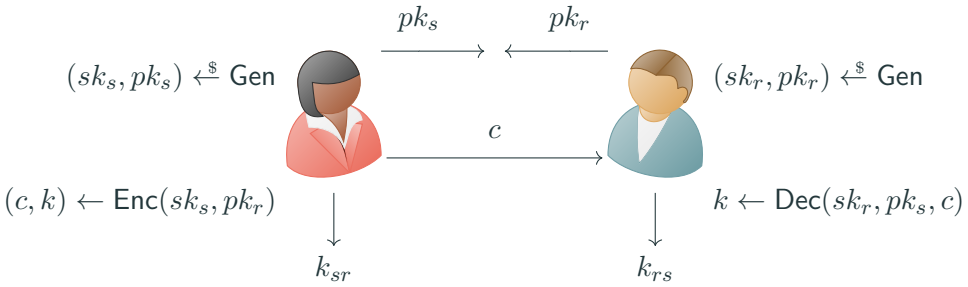

pk_s
pk_r
$(sk_s, pk_s) \xleftarrow{\$} \mathsf{Gen}$
$(sk_r, pk_r) \xleftarrow{\$} \mathsf{Gen}$
$(c, k) \leftarrow \mathsf{Enc}(sk_s, pk_r)$


pk_s
pk_r
$(sk_s, pk_s) \xleftarrow{\$} \mathsf{Gen}$
$(sk_r, pk_r) \xleftarrow{\$} \mathsf{Gen}$
c
$(c, k) \leftarrow \mathsf{Enc}(sk_s, pk_r)$

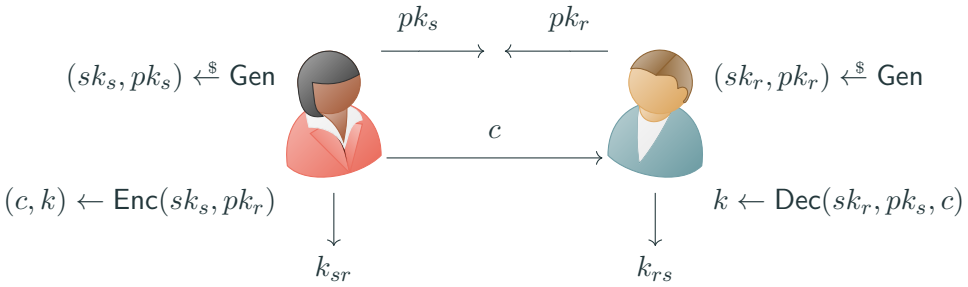

pk_s
pk_r
$(sk_s, pk_s) \xleftarrow{\$} \mathsf{Gen}$
$(sk_r, pk_r) \xleftarrow{\$} \mathsf{Gen}$
c
$(c, k) \leftarrow \mathsf{Enc}(sk_s, pk_r)$
$k \leftarrow \mathsf{Dec}(sk_r, pk_s, c)$

AUTHENTICATED KEY ENCAPSULATION MECHANISM (AKEM) [ABH+21]

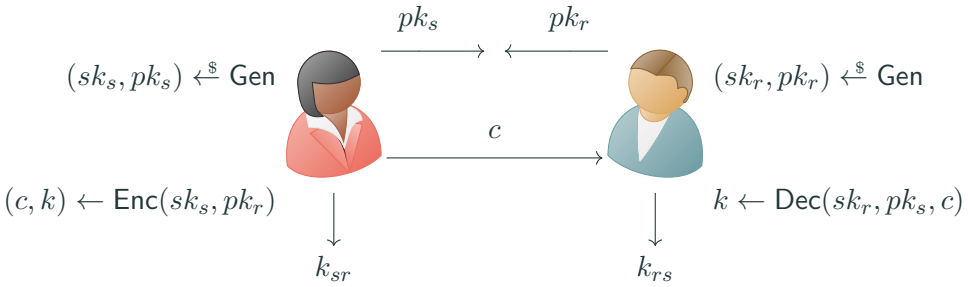




- **Confidentiality:** k_{sr} and k_{rs} should look random. ✓



- **Confidentiality:** k_{sr} and k_{rs} should look random. ✓
- **Authenticity:** r knows s sent the ciphertext c. ✓



- **Confidentiality:** k_{sr} and k_{rs} should look random. ✓
- **Authenticity:** r knows s sent the ciphertext c. ✓
- **Deniability:** s can deny having sent c to r.

$b \xleftarrow{\$} \{0,1\}$

$b \xleftarrow{\$} \{0,1\}$

$\downarrow$

b'

$b \xleftarrow{\$} \{0,1\}$

$\downarrow$

b'

if $b = b'$

return win

$b \xleftarrow{\$} \{0,1\}$

$pk_1, \ldots, pk_n \longrightarrow$

b'

if $b = b'$

return win

$b \xleftarrow{\$} \{0,1\}$

$pk_1, \ldots, pk_n \longrightarrow$

$\texttt{Chall}(s \in [n], r \in [n]) \longleftarrow$

$\downarrow b'$

if $b = b'$

return win

$b \xleftarrow{\$} \{0,1\}$

$pk_1, \ldots, pk_n$ →

if $b = 0$

$(c, k) \xleftarrow{\$} \mathsf{Enc}(sk_s, pk_r)$

if $b = 1$

$(c, k) \xleftarrow{\$} \mathsf{Sim}(\ldots)$

$\texttt{Chall}(s \in [n], r \in [n])$ ←

(c, k) →

b'

if $b = b'$

return win

$b \xleftarrow{\$} \{0,1\}$

$pk_1, \ldots, pk_n$ →

if $b = 0$

$(c, k) \xleftarrow{\$} \mathsf{Enc}(sk_s, pk_r)$

if $b = 1$

$(c, k) \xleftarrow{\$} \mathsf{Sim}(\ldots)$

$\texttt{Chall}(s \in [n], r \in [n])$ ←

(c, k) →

if $b = b'$

return win

b'

$b \xleftarrow{\$} \{0,1\}$

$pk_1, \ldots, pk_n$

$\ldots$

if $b = 0$

$(c, k) \xleftarrow{\$} \mathsf{Enc}(sk_s, pk_r)$

if $b = 1$

$(c, k) \xleftarrow{\$} \mathsf{Sim}(\ldots)$

$\texttt{Chall}(s \in [n], r \in [n])$

(c, k)

if $b = b'$

return win

b'

Honest Sender					

		Honest Receiver		Dishonest Receiver	
Honest Sender					

		Honest Receiver		Dishonest Receiver	
Honest Sender		$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(\emptyset)$		
		$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(\emptyset)$		

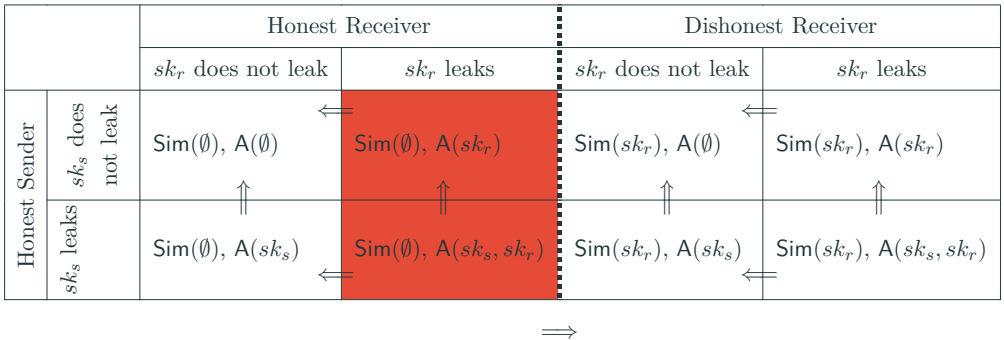
		Honest Receiver		Dishonest Receiver	
Honest Sender		$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(sk_r)$	$\mathsf{Sim}(sk_r)$
		$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(sk_r)$	$\mathsf{Sim}(sk_r)$

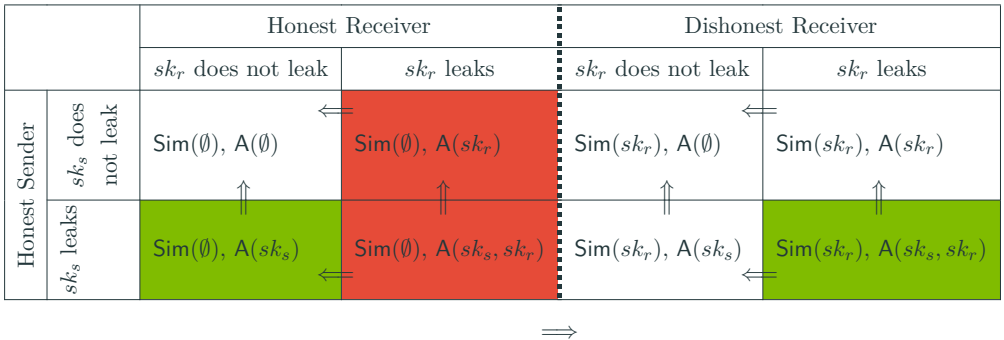
		Honest Receiver		Dishonest Receiver	
		sk_r does not leak		sk_r does not leak	
Honest Sender	sk_s does not leak	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(\emptyset)$	$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(\emptyset)$	$\mathsf{Sim}(sk_r)$
		$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(sk_r)$	$\mathsf{Sim}(sk_r)$

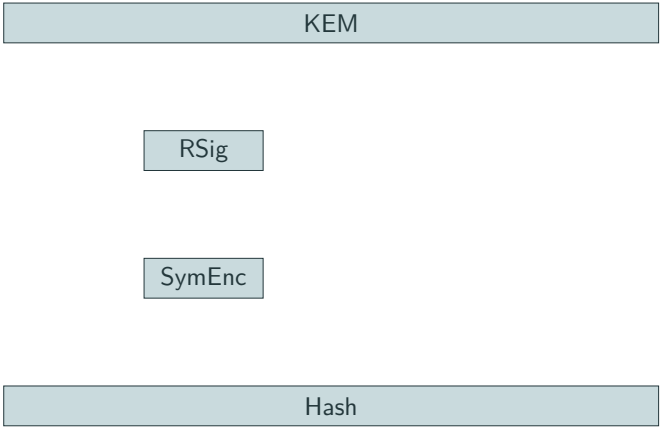
		Honest Receiver		Dishonest Receiver	
		sk_r does not leak		sk_r does not leak	
Honest Sender	sk_s does not leak	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(\emptyset)$	$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(\emptyset)$	$\mathsf{Sim}(sk_r)$
	sk_s leaks	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(sk_s)$	$\mathsf{Sim}(\emptyset)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(sk_s)$	$\mathsf{Sim}(sk_r)$

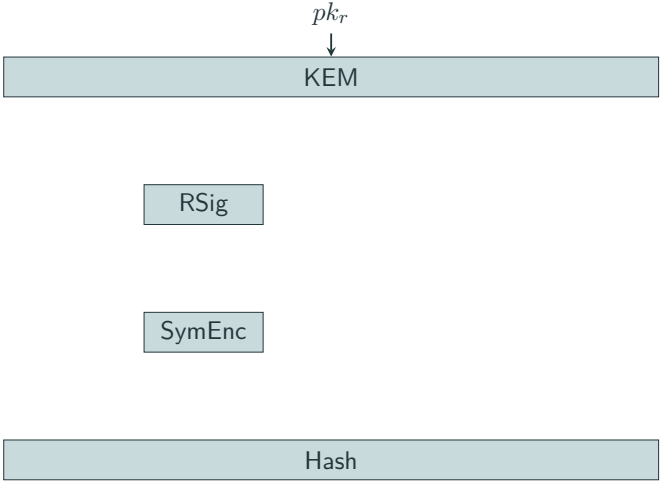
		Honest Receiver		Dishonest Receiver	
		sk_r does not leak	sk_r leaks	sk_r does not leak	sk_r leaks
Honest Sender	sk_s does not leak	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(\emptyset)$	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(sk_r)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(\emptyset)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(sk_r)$
	sk_s leaks	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(sk_s)$	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(sk_s, sk_r)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(sk_s)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(sk_s, sk_r)$

		Honest Receiver		Dishonest Receiver	
		sk_r does not leak	sk_r leaks	sk_r does not leak	sk_r leaks
Honest Sender	sk_s does not leak	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(\emptyset)$	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(sk_r)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(\emptyset)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(sk_r)$
	sk_s leaks	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(sk_s)$	$\mathsf{Sim}(\emptyset)$, $\mathsf{A}(sk_s, sk_r)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(sk_s)$	$\mathsf{Sim}(sk_r)$, $\mathsf{A}(sk_s, sk_r)$

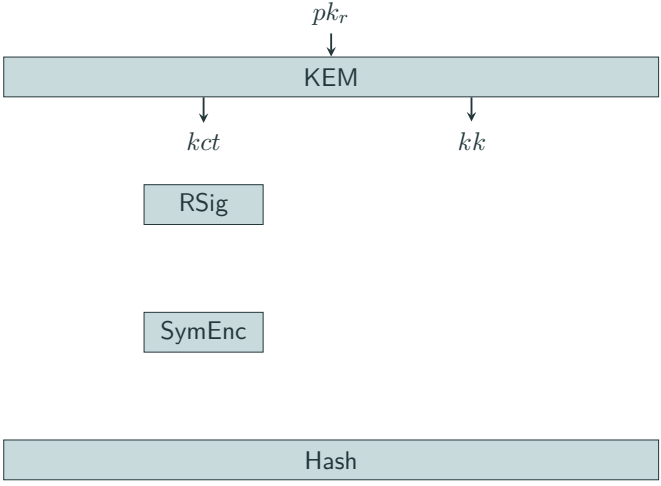

Honest Receiver
Dishonest Receiver
sk_r does not leak
sk_r leaks
sk_r does not leak
sk_r leaks
Honest Sender
sk_s does not leak
sk_s leaks
Sim(∅), A(∅)
Sim(∅), A(sk_r)
Sim(sk_r), A(∅)
Sim(sk_r), A(sk_r)
Sim(∅), A(sk_s)
Sim(∅), A(sk_s, sk_r)
Sim(sk_r), A(sk_s)
Sim(sk_r), A(sk_s, sk_r)


Honest Receiver
Dishonest Receiver
sk_r does not leak
sk_r leaks
sk_r does not leak
sk_r leaks
Honest Sender
sk_s does not leak
sk_s leaks
Sim(∅), A(∅)
Sim(∅), A(sk_r)
Sim(sk_r), A(∅)
Sim(sk_r), A(sk_r)
Sim(∅), A(sk_s)
Sim(∅), A(sk_s, sk_r)
Sim(sk_r), A(sk_s)
Sim(sk_r), A(sk_s, sk_r)

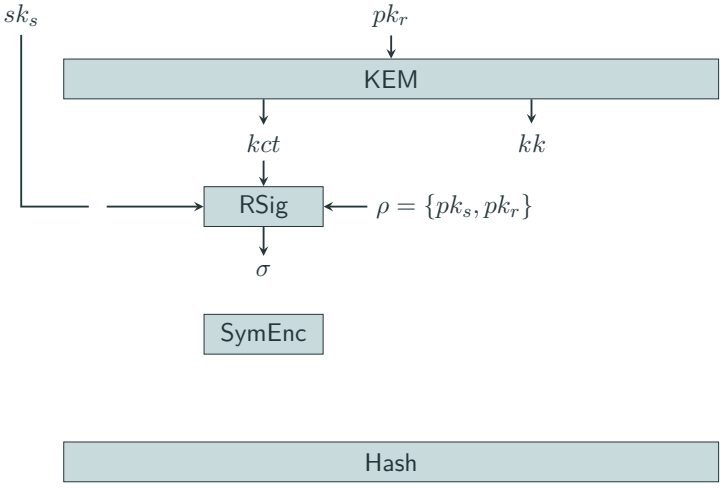

KEM
RSig
SymEnc
Hash


pk_r
KEM
RSig
SymEnc
Hash

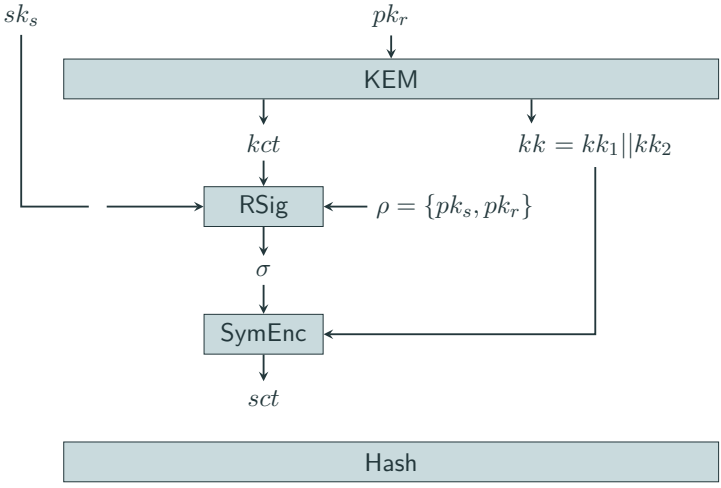
DENIABLE AKEM: BLACK-BOX CONSTRUCTION



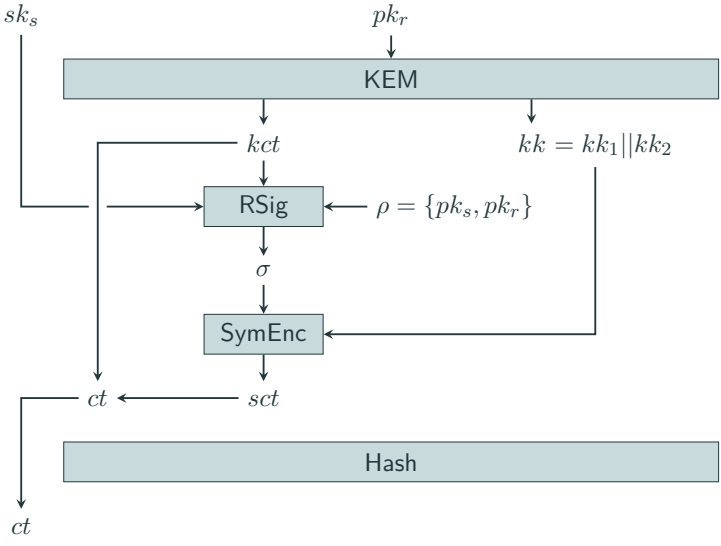
DENIABLE AKEM: BLACK-BOX CONSTRUCTION



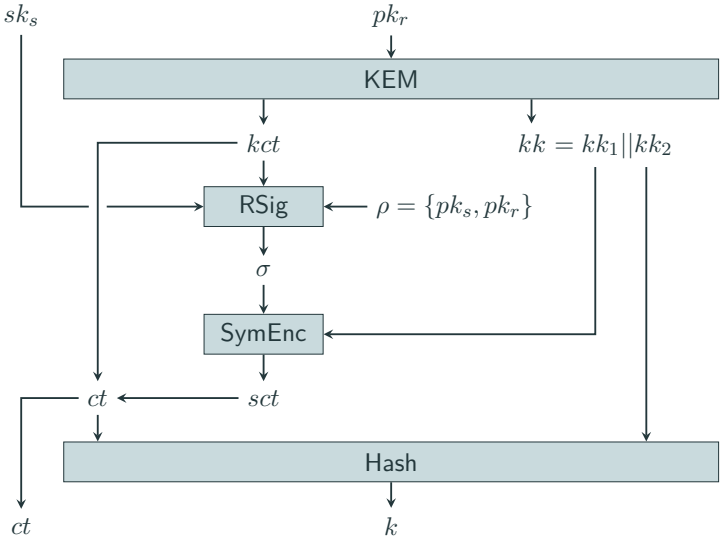
DENIABLE AKEM: BLACK-BOX CONSTRUCTION



DENIABLE AKEM: BLACK-BOX CONSTRUCTION



DENIABLE AKEM: BLACK-BOX CONSTRUCTION



AKEM COMPARISON

Scheme (variant)	Confidentiality	Authenticity	Deniability	PQ	Size (in bytes)	
					c	pk
DH-AKEM (`Curve25519`) [ABH+21]	**Ins-CCA**	**Out-Aut**	**DR-Den**[*]	✗	32	32
EtStH-AKEM (NTRU-A + ANTRAG) [AJKL23]	**Ins-CCA**	**Out-Aut**	—	✓	1 414	1 664
NIKE-AKEM (SWOOSH[1]) [AJKL23]	**Ins-CCA**	**Out-Aut**	**DR-Den**[*]	✓	$> 221\,184$	$> 221\,184$
FrodoKEX+ [CHDN+24]	**IND-1BatchCCA**	**UNF-1KCA**	**DR-Den**	✓	72	21 300
THIS WORK (NTRU-A + GANDALF)	**Ins-CCA**	**Out-Aut**	**HR-Den & DR-Den**	✓	2 004	1 664

SUMMARY

Contributions:

- Gandalf an NTRU-based ring signature scheme:
  - 50% reduction in signature size compared to Raptor [LAZ19].
  - For rings of size two, $|\sigma| = 1236$ bytes, a quarter the size of DualRing [YEL+21].
- Formalised deniability for AKEM, the primitive behind HPKE used in MLS.
- Black-box construction of deniable AKEM:
  - Ciphertext size of 2004 bytes when instantiated with Gandalf.

ia.cr/2024/890

phillip.gajland@{mpi-sp.org,rub.de}
p4i11ip

Contributions:

- Gandalf an NTRU-based ring signature scheme:
  - 50% reduction in signature size compared to Raptor [LAZ19].
  - For rings of size two, $|\sigma| = 1236$ bytes, a quarter the size of DualRing [YEL+21].
- Formalised deniability for AKEM, the primitive behind HPKE used in MLS.
- Black-box construction of deniable AKEM:
  - Ciphertext size of 2004 bytes when instantiated with Gandalf.

ia.cr/2024/890

phillip.gajland@{mpi-sp.org,rub.de}
p4i11ip

Contributions:

- Gandalf an NTRU-based ring signature scheme:
  - 50% reduction in signature size compared to Raptor [LAZ19].
  - For rings of size two, $|\sigma| = 1236$ bytes, a quarter the size of DualRing [YEL+21].
- Formalised deniability for AKEM, the primitive behind HPKE used in MLS.
- Black-box construction of deniable AKEM:
  - Ciphertext size of 2004 bytes when instantiated with Gandalf.

ia.cr/2024/890

phillip.gajland@{mpi-sp.org,rub.de}
p4i11ip

Contributions:

- Gandalf an NTRU-based ring signature scheme:
  - 50% reduction in signature size compared to Raptor [LAZ19].
  - For rings of size two, $|\sigma| = 1236$ bytes, a quarter the size of DualRing [YEL+21].
- Formalised deniability for AKEM, the primitive behind HPKE used in MLS.
- Black-box construction of deniable AKEM:
  - Ciphertext size of 2004 bytes when instantiated with Gandalf.

ia.cr/2024/890

phillip.gajland@{mpi-sp.org,rub.de}
p4i11ip

Contributions:

- Gandalf an NTRU-based ring signature scheme:
  - 50% reduction in signature size compared to Raptor [LAZ19].
  - For rings of size two, $|\sigma| = 1236$ bytes, a quarter the size of DualRing [YEL+21].
- Formalised deniability for AKEM, the primitive behind HPKE used in MLS.
- Black-box construction of deniable AKEM:
  - Ciphertext size of 2004 bytes when instantiated with Gandalf.

ia.cr/2024/890

phillip.gajland@{mpi-sp.org,rub.de}
p4i11ip

Contributions:

- Gandalf an NTRU-based ring signature scheme:
  - 50% reduction in signature size compared to Raptor [LAZ19].
  - For rings of size two, $|\sigma| = 1236$ bytes, a quarter the size of DualRing [YEL+21].
- Formalised deniability for AKEM, the primitive behind HPKE used in MLS.
- Black-box construction of deniable AKEM:
  - Ciphertext size of 2004 bytes when instantiated with Gandalf.

ia.cr/2024/890

phillip.gajland@{mpi-sp.org,rub.de}
p4i11ip

Contributions:

- Gandalf an NTRU-based ring signature scheme:
  - 50% reduction in signature size compared to Raptor [LAZ19].
  - For rings of size two, $|\sigma| = 1236$ bytes, a quarter the size of DualRing [YEL+21].
- Formalised deniability for AKEM, the primitive behind HPKE used in MLS.
- Black-box construction of deniable AKEM:
  - Ciphertext size of 2004 bytes when instantiated with Gandalf.

ia.cr/2024/890

phillip.gajland@{mpi-sp.org,rub.de}

p4i11ip

REFERENCES I

[ABH+21] Joël Alwen, Bruno Blanchet, Eduard Hauck, Eike Kiltz, Benjamin Lipp, and Doreen Riepel. Analysing the HPKE standard. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 87–116, Zagreb, Croatia, October 17–21, 2021. Springer, Cham, Switzerland.

[AJKL23] Joël Alwen, Jonas Janneck, Eike Kiltz, and Benjamin Lipp. The pre-shared key modes of HPKE. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology – ASIACRYPT 2023, Part VI*, volume 14443 of *Lecture Notes in Computer Science*, pages 329–360, Guangzhou, China, December 4–8, 2023. Springer, Singapore, Singapore.

[BBLW22] Richard Barnes, Karthikeyan Bhargavan, Benjamin Lipp, and Christopher A. Wood. Hybrid Public Key Encryption. RFC 9180, February 2022.

[BBR+23] Richard Barnes, Benjamin Beurdouche, Raphael Robert, Jon Millican, Emad Omara, and Katriel Cohn-Gordon. The Messaging Layer Security (MLS) Protocol. RFC 9420, July 2023.

[CHDN+24] Daniel Collins, Loïs Huguenin-Dumittan, Ngoc Khanh Nguyen, Nicolas Rolin, and Serge Vaudenay. K-waay: Fast and deniable post-quantum x3dh without ring signatures. Cryptology ePrint Archive, Paper 2024/120, 2024. https://eprint.iacr.org/2024/120.

[LAZ19] Xingye Lu, Man Ho Au, and Zhenfei Zhang. Raptor: A practical lattice-based (linkable) ring signature. In Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa, and Moti Yung, editors, *ACNS 19: 17th International Conference on Applied Cryptography and Network Security*, volume 11464 of *Lecture Notes in Computer Science*, pages 110–130, Bogota, Colombia, June 5–7, 2019. Springer, Cham, Switzerland.

[LDK+22] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

REFERENCES II

[LNS21] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler. SMILE: Set membership from ideal lattices with applications to ring signatures and confidential transactions. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021, Part II*, volume 12826 of *Lecture Notes in Computer Science*, pages 611–640, Virtual Event, August 16–20, 2021. Springer, Cham, Switzerland.

[RST01] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565, Gold Coast, Australia, December 9–13, 2001. Springer, Berlin, Heidelberg, Germany.

[SAB+22] Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehlé, and Jintai Ding. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[YEL+21] Tsz Hon Yuen, Muhammed F. Esgin, Joseph K. Liu, Man Ho Au, and Zhimin Ding. DualRing: Generic construction of ring signatures with efficient instantiations. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 251–281, Virtual Event, August 16–20, 2021. Springer, Cham, Switzerland.

Gandalf parameters

Parameter	Description	Value
N	dimension of $\mathcal{R} \coloneqq \mathbb{Z}[X]/(X^N+1)$	512
ϵ	Smoothing parameter order	$\frac{1}{\sqrt{Q_{\text{sgn}} \cdot \lambda}}$
δ_{KL}	maximum KL-divergence of PreSmp	2ϵ
a	Rényi order	2λ
R_a	maximum Rényi divergence of PreSmp	$1 + 2a\epsilon^2$
α	quality of NTRU trapdoor	1.15
q	prime modulus	12289
s	standard deviation of Gaussian sampler	$\frac{1}{\pi} \cdot \sqrt{\frac{\ln(4N(1+1/\epsilon))}{2}} \cdot \alpha \cdot \sqrt{q}$
τ	tailcut rate of signatures	$[1.08, 1.22]$
κ	maximum size of signing ring	≥ 2
$\lvert\rho\rvert = k$	size of signing ring	$[2, \kappa]$
β	maximum norm of signatures	$\tau \cdot s \cdot \sqrt{(\kappa+1)N}$
$\lvert pk\rvert$	verification key size (bytes)	896
$\lvert\sigma\rvert$	signature size (bytes)	$606 \cdot k + 24$