k-times Full Traceable Ring Signature

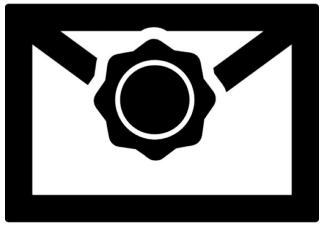
Xavier Bultel **Pascal Lafourcade**

31 August 2016,

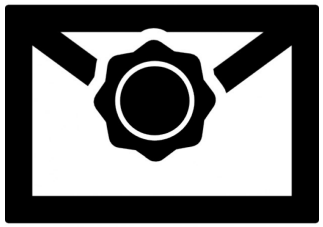
ARES Conference

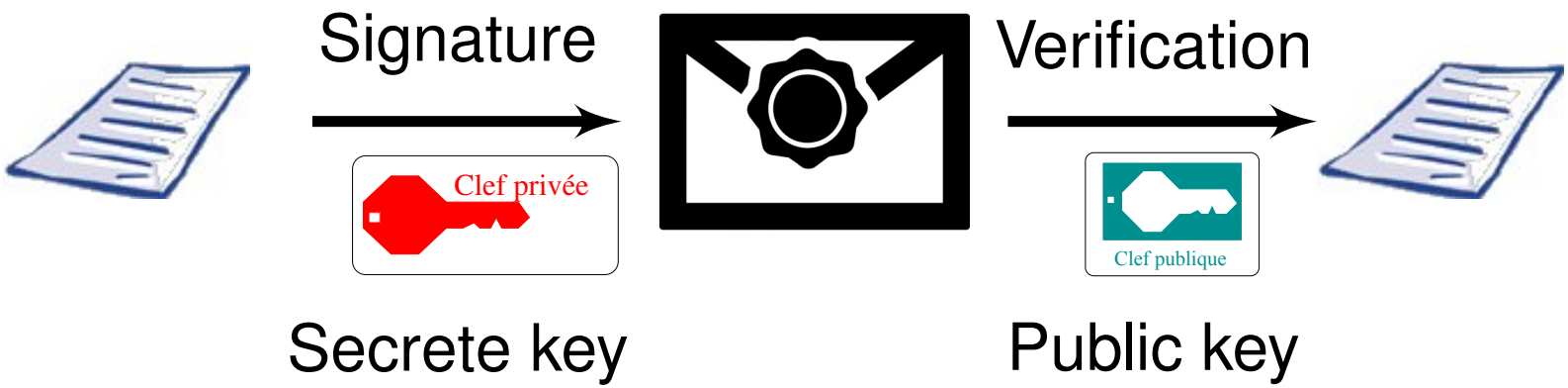
International Conference on Availability, Reliability and Security

Signature



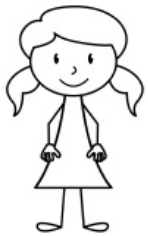
Signature





1977, RSA: $m^d \mod n$

Ring Signature (Rivest *et al.*, 2001)

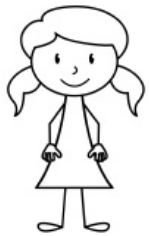
Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

σ_1, σ_2, σ_3, σ_4, σ_5, σ_6 and σ_7 come from **Alice or Bob or Carol or David**

$\rightarrow$ Anonymous signatures

Linkable Signature (Liu *et al.*, 2004)

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

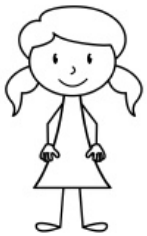
σ_1, σ_2 and σ_3 come from **the same user**

σ_5 and σ_6 come from **the same user**

No information about σ_4 and σ_7 signer

$\rightarrow$ Anonymous but Linkable

1-time Traceable Sig. (Canard *et al.*, 2006)

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

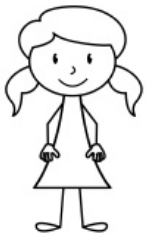
σ_1, σ_2 and σ_3 comes from **Alice**

σ_5 and σ_6 comes from **Carol**

σ_4 and σ_7 are **anonymous**

$\rightarrow$ Only 1 anonymous signature per group member

2-times Traceable Sig. (Au *et al.*, 2006)

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

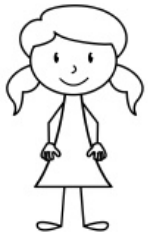
Observer

σ_1 and σ_3 comes from **Alice**

$\sigma_2, \sigma_4, \sigma_5, \sigma_6$ and σ_7 are **anonymous**

$\rightarrow$ Only 2 anonymous signature

2-times Traceable Sig. (Au *et al.*, 2006)

Alice  (m_1, σ_1) $\boxed{(m_2, \sigma_2)}$ (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

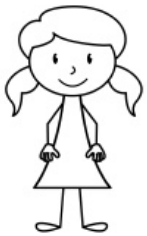
σ_1 and σ_3 comes from **Alice**

$\boxed{\sigma_2}$, σ_4, σ_5, σ_6 and σ_7 are **anonymous**

$\rightarrow$ Only 2 anonymous signature

$\boxed{\sigma_2 \text{ is anonymous} \rightarrow \text{not full traceable}}$

Our contribution: k-times Full Traceable Sig.

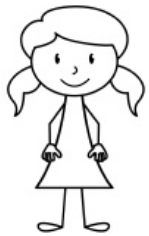
Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

σ_1, σ_2 and σ_3 comes from **Alice**

σ_4, σ_5, σ_6 and σ_7 are **anonymous**

Our contribution: k-times Full Traceable Sig.

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

σ_1, σ_2 and σ_3 comes from **Alice**

σ_4, σ_5, σ_6 and σ_7 are **anonymous**

$\rightarrow$ k anonymous signature per users

$\rightarrow$ Trace all cheater's signatures

Our contributions

k-times Full Traceable Signature

- Generalize traceable signatures
- Ring signature (ad-hoc group)
- Event oriented
- Fine-grained k
- Anonymous (less than k)
- Full public linkability (more than k)
- Full public traceability (more than k)

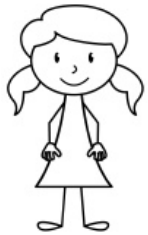
Applications:

1. proxy voting
2. k-times veto

Application in k-times Veto for CARS'16


Alice


Bob


Carol


David

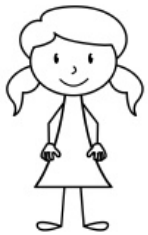
Conference on Anonymous Ring Signatures

- **List of *candidates*** for the Program Commitee (PC): Albert, Bernard, Cedric, Donald, Edward, Fabien, Gaston, Hercul, Ivan, Jim, Karl
- Each member of Steering Commitee (SC) can **exclude** k **names** of the list
- Vetos are **anonymous**
- Members who exceed this limitation are **excluded** and their vetos are discarded

Application: k-times Veto

PC= Albert, Bernard, Cedric, Donald, Edward, Fabien, Gaston, Hercul, Ivan, Jim, Karl

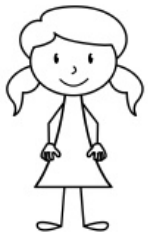
Veto using 2-times traceable signature:

Alice 	(Donald, σ(Donald)) (Jim, σ(Jim)) (Edward, σ(Edward))
Bob 	(Edward, σ(Edward))
Carol 	(Albert, σ(*Albert*)) (Gaston, σ(Gaston))
David 	(Gaston, σ(Gaston))

Application: k-times Veto

PC= Albert, Bernard, Cedric, Donald, Edward, Fabien, Gaston, Hercul, Ivan, Jim, Karl

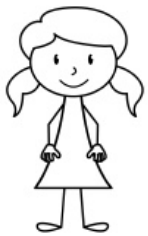
Veto using 2-times traceable signature:

~~Alice~~ 	~~(Donald, σ(Donald))~~ (Jim, σ(Jim)) ~~(Edward, σ(Edward))~~
Bob 	(Edward, σ(Edward))
Carol 	(Albert, σ(*Albert*)) (Gaston, σ(Gaston))
David 	(Gaston, σ(Gaston))

Application: k-times Veto

PC= Albert, Bernard, Cedric, Donald, Edward, Fabien, Gaston, Hercul, Ivan, Jim, Karl

Veto using 2-times full traceable signature:

~~Alice~~ 	~~(Donald, σ(Donald))~~ ~~(Jim, σ(Jim))~~ ~~(Edward, σ(Edward))~~
Bob 	(Edward, σ(Edward))
Carol 	(Albert, σ(*Albert*)) (Gaston, σ(Gaston))
David 	(Gaston, σ(Gaston))

Outline

Outline

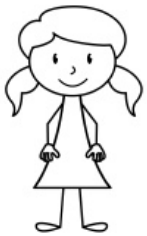
Formal Definition

L, L_1 and L_2 are sets of public keys (identities) of users' ring

Definition (k-FTRS)

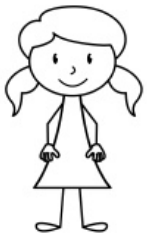
$\text{Init}(1^t)$:	output init
$\text{Gen}(\text{init}, k)$:	output a signing key pair (ssk, svk)
$\text{Sig}_E(\text{ssk}, m, L, j)$:	output a signature σ
$\text{Ver}_E(L, \sigma, m)$:	check that σ is valid
$\text{Link}_E(L_1, L_2, \sigma_1, \sigma_2, m_1, m_2)$:	test link between σ_1 and σ_2
$\text{Match}_E(L_1, L_2, \sigma_1, \sigma_2, m_1, m_2)$:	output svk_u and a tracer $\omega_{(E,u)}$
$\text{Trace}_E(L, \sigma, m, \omega_{(E,u)})$:	check whether σ comes from the user u.

Example (2-times)

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

Example (2-times)

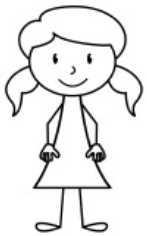
Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

Detect cheaters: link on all pairs (σ_i, σ_j)

$\rightarrow$ Link σ_1 and σ_3

Example (2-times)

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

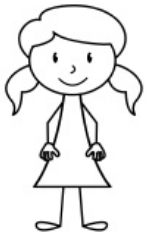
Detect cheaters: link on all pairs (σ_i, σ_j)

$\rightarrow$ Link σ_1 and σ_3

Identify cheater: match on σ_1 and σ_3

$\rightarrow$ $\text{svk}_{\text{alice}}$ and tracer ω

Example (2-times)

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

Detect cheaters: link on all pairs (σ_i, σ_j)

$\rightarrow$ Link σ_1 and σ_3

Identify cheater: match on σ_1 and σ_3

$\rightarrow$ $\text{svk}_{\text{alice}}$ and tracer ω

Remove signature: trace using ω on all σ

$\rightarrow$ Trace and remove σ_2

Security

Definition (Unforgeability)

- It is infeasible to **forge a signature** without the key
- Signature oracle

Security

Definition (Unforgeability)

- It is infeasible to **forge a signature** without the key
- Signature oracle

Definition (Anonymity)

- It is infeasible to **guess the identity of a signer** from less than k signatures
- Signature oracle (with inherent restrictions)

Security

Definition (Unforgeability)

- It is infeasible to **forge a signature** without the key
- Signature oracle

Definition (Anonymity)

- It is infeasible to **guess the identity of a signer** from less than k signatures
- Signature oracle (with inherent restrictions)

Definition (Traceability)

- More than k signatures are **always traceable**
- Signature oracle

Outline

Idea of Construction

- Inspired of **Canard *et al.*** (1-time traceable)
- **ZKP of correctness** of the signature
- **Identity is *"encrypted"*** in signatures
- **Match algorithm** outputs a key (tracer) that allows to **decrypt identity**

Cryptographic Assumptions

- Bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_t$ in $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, g_1, g_2)$:

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$$

- DDH assumption:
  - **Instance**: g_1^a, g_1^b and g_1^z
  - **Problem**: $z = ab$ or not?
- BDDH assumption:
  - **Instance**: g_1^a, g_1^b, g_2^c and $e(g_1, g_2)^z$
  - **Problem**: $z = abc$ or not?
- 2BDDH assumption:
  - **Instance**: g_1^a, g_1^b, g_2^c, g_2^d, $e(g_1, g_2)^{abc}$ and $e(g_1, g_2)^z$
  - **Problem**: $z = abd$ or not?

Signature Construction (i-times) with $i = 2$

- **Secret key:** x_1, x_2 and x
- **Public key:** $g_1^{x_1}, g_1^{x_2}$ and g_1^{x}
- **Event:** $E \in \{0,1\}^*$; H_0 and H_1 two hash functions

Signature Construction (i-times) with $i = 2$

- **Secret key:** x_1, x_2 and x
- **Public key:** $g_1^{x_1}, g_1^{x_2}$ and g_1^{x}
- **Event:** $E \in \{0,1\}^*$; H_0 and H_1 two hash functions

The signer picks $i \xleftarrow{\$} \{1,2\}$, $r \xleftarrow{\$} \mathbb{Z}_p^*$ and computes:

$$A = \mathrm{H}_0(E, 0) \qquad B = \mathrm{H}_0(E, 1)$$
$$C = \mathrm{H}_0(E, 2) \qquad W = \mathrm{H}_0(E, 3)$$
$$u = \mathrm{H}_1(E, m, 0, g_2^r) \qquad v = H_1(E, m, 1, g_2^r)$$

Then he computes the signature $\sigma = (T_1, T_2, T_3, T_4, T_5, T_6)$:

$$T_1 = A^{x_i} \qquad T_2 = B^{x_i} \cdot {g_1}^{x \cdot u}$$
$$T_3 = C^{x_i} \cdot W^{v \cdot x} \qquad T_4 = g_2^r$$
$$T_5 = e(W, T_4)^x \qquad T_6 = \text{ZKP of correctness of } \sigma$$

Signature Construction (2-times)

- **Secret key:** x_1, x_2 and x
- **Public key:** $g_1^{x_1}, g_1^{x_2}$ and g_1^{x}

$$\sigma = (T_1, T_2, T_3, T_4, T_5, T_6)$$

$$T_1 = A^{x_i} \qquad T_2 = B^{x_i} \cdot g_1{}^{x \cdot u}$$
$$T_3 = C^{x_i} \cdot W^{v \cdot x} \qquad T_4 = g_2^{r}$$
$$T_5 = e(W, T_4)^{x} \qquad T_6 = \text{ZKP of correctness of } \sigma$$

Unforgeability:

Validity of ZKP: Without (x_1, x_2, x), impossible to forge T_6

Signature Construction (2-times)

- **Secret key:** x_1, x_2 and x
- **Public key:** $g_1^{x_1}, g_1^{x_2}$ and g_1^{x}

$$T_1 = A^{x_i} \qquad T_2 = B^{x_i} \cdot {g_1}^{x \cdot u}$$
$$T_3 = C^{x_i} \cdot W^{v \cdot x} \qquad T_4 = g_2^{r}$$
$$T_5 = e(W, T_4)^{x} \qquad T_6 = \text{ZKP of correctness of } \sigma$$

Anonymity:

- T_1: DDH with $(A, g_1^{x_i}, A^{x_i})$
- T_2: DDH with $(B, g_1^{x_i}, B^{x_i})$
- T_3: DDH with $(C, g_1^{x_i}, C^{x_i})$
- T_5: BDDH with $(W, T_4, g^{x}, e(W, T_4)^{x})$
- T_6: zero-knowlege

Signature Construction (2-times)

Secret key: x_1, x_2 and x; **Public key:** $g_1^{x_1}, g_1^{x_2}$ and g_1^{x}

$T\ (i=1)$	$T'\ (i=2)$	$T''\ (i=1)$
$T_1 = A^{x_1}$	$T'_1 = A^{x_2}$	$T''_1 = A^{x_1}$
$T_2 = B^{x_1} \cdot {g_1}^{x \cdot u}$	$T'_2 = B^{x_2} \cdot {g_1}^{x \cdot u'}$	$T''_2 = B^{x_1} \cdot {g_1}^{x \cdot u''}$
$T_3 = C^{x_1} \cdot W^{v \cdot x}$	$T'_3 = C^{x_2} \cdot W^{v' \cdot x}$	$T''_3 = C^{x_1} \cdot W^{v'' \cdot x}$
$T_4 = g_2^{r}$	$T'_4 = g_2^{r'}$	$T''_4 = g_2^{r''}$
$T_5 = e(W, T_4)^{x}$	$T'_5 = e(W, T'_4)^{x}$	$T''_5 = e(W, T''_4)^{x}$

Signature Construction (2-times)

Secret key: x_1, x_2 and x; **Public key:** $g_1^{x_1}, g_1^{x_2}$ and g_1^{x}

$T\ (i=1)$	$T'\ (i=2)$	$T''\ (i=1)$
$T_1 = A^{x_1}$	$T'_1 = A^{x_2}$	$T''_1 = A^{x_1}$
$T_2 = B^{x_1} \cdot {g_1}^{x \cdot u}$	$T'_2 = B^{x_2} \cdot {g_1}^{x \cdot u'}$	$T''_2 = B^{x_1} \cdot {g_1}^{x \cdot u''}$
$T_3 = C^{x_1} \cdot W^{v \cdot x}$	$T'_3 = C^{x_2} \cdot W^{v' \cdot x}$	$T''_3 = C^{x_1} \cdot W^{v'' \cdot x}$
$T_4 = g_2^{r}$	$T'_4 = g_2^{r'}$	$T''_4 = g_2^{r''}$
$T_5 = e(W, T_4)^{x}$	$T'_5 = e(W, T'_4)^{x}$	$T''_5 = e(W, T''_4)^{x}$

LINK: T and T'' are linkable: check that $T_1 = T''_1$

Signature Construction (2-times)

Secret key: x_1, x_2 and x; **Public key:** $g_1^{x_1}, g_1^{x_2}$ and g_1^{x}

$T\ (i=1)$	$T'\ (i=2)$	$T''\ (i=1)$
$T_1 = A^{x_1}$	$T'_1 = A^{x_2}$	$T''_1 = A^{x_1}$
$T_2 = B^{x_1} \cdot {g_1}^{x \cdot u}$	$T'_2 = B^{x_2} \cdot {g_1}^{x \cdot u'}$	$T''_2 = B^{x_1} \cdot {g_1}^{x \cdot u''}$
$T_3 = C^{x_1} \cdot W^{v \cdot x}$	$T'_3 = C^{x_2} \cdot W^{v' \cdot x}$	$T''_3 = C^{x_1} \cdot W^{v'' \cdot x}$
$T_4 = g_2^{r}$	$T'_4 = g_2^{r'}$	$T''_4 = g_2^{r''}$
$T_5 = e(W, T_4)^{x}$	$T'_5 = e(W, T'_4)^{x}$	$T''_5 = e(W, T''_4)^{x}$

MATCH: T **and** T''

$$\left(\frac{T_2}{T''_2}\right)^{\frac{1}{u-u''}} = \left(\frac{B^{x_1} \cdot g_1^{x \cdot u}}{B^{x_1} \cdot g_1^{x \cdot u''}}\right)^{\frac{1}{u-u''}} = g_1^{x}; \quad \left(\frac{T_3}{T''_3}\right)^{\frac{1}{v-v''}} = W^{x} = \omega$$

Signature Construction (2-times)

Secret key: x_1, x_2 and x; **Public key:** $g_1^{x_1}, g_1^{x_2}$ and g_1^{x}

$T\ (i=1)$	$T'\ (i=2)$	$T''\ (i=1)$
$T_1 = A^{x_1}$	$T'_1 = A^{x_2}$	$T''_1 = A^{x_1}$
$T_2 = B^{x_1} \cdot {g_1}^{x \cdot u}$	$T'_2 = B^{x_2} \cdot {g_1}^{x \cdot u'}$	$T''_2 = B^{x_1} \cdot {g_1}^{x \cdot u''}$
$T_3 = C^{x_1} \cdot W^{v \cdot x}$	$T'_3 = C^{x_2} \cdot W^{v' \cdot x}$	$T''_3 = C^{x_1} \cdot W^{v'' \cdot x}$
$T_4 = g_2^{r}$	$T'_4 = g_2^{r'}$	$T''_4 = g_2^{r''}$
$T_5 = e(W, T_4)^{x}$	$T'_5 = e(W, T'_4)^{x}$	$T''_5 = e(W, T''_4)^{x}$

TRACE: T using the tracer $\omega = W^x$, check that:

$$e(\omega, T'_4) = T'_5$$

Signature Construction (2-times)

Secret key: x_1, x_2 and x; **Public key:** $g_1^{x_1}, g_1^{x_2}$ and g_1^{x}

$T\ (i=1)$	$T'\ (i=2)$	$T''\ (i=1)$
$T_1 = A^{x_1}$	$T'_1 = A^{x_2}$	$T''_1 = A^{x_1}$
$T_2 = B^{x_1} \cdot {g_1}^{x \cdot u}$	$T'_2 = B^{x_2} \cdot {g_1}^{x \cdot u'}$	$T''_2 = B^{x_1} \cdot {g_1}^{x \cdot u''}$
$T_3 = C^{x_1} \cdot W^{v \cdot x}$	$T'_3 = C^{x_2} \cdot W^{v' \cdot x}$	$T''_3 = C^{x_1} \cdot W^{v'' \cdot x}$
$T_4 = g_2^{r}$	$T'_4 = g_2^{r'}$	$T''_4 = g_2^{r''}$
$T_5 = e(W, T_4)^{x}$	$T'_5 = e(W, T'_4)^{x}$	$T''_5 = e(W, T''_4)^{x}$

Traceability:

If signatures are **well formed**, link, match and trace work
$\rightarrow$ **Validity** of the ZKP of correctness

Security Analysis

Theorem

*Our k-FTRS scheme is **unforgeable**, **traceable** and **anonymous** under the DDH assumption in $\mathbb{G}_1$ and the 2BDDH assumption in the random oracle model*

Outline

Conclusion

Comparaison:

Schemes	Sig. size	Ad-hoc	Times	Trac.	Full trac.
Ring signature	$O(n)$	Yes	∞	-	-
Short group sig.	$O(1)$	No	∞	-	-
Linkable sig.	$O(n)$	Yes	1	No	-
List sig. (Ad-hoc)	$O(n)$	Yes	1	Yes	-
k-times group sig.	$O(1)$	No	k	Yes	No
Ktrace	$\mathbf{O(n \cdot k)}$	**Yes**	k	**Yes**	**Yes**

Conclusion

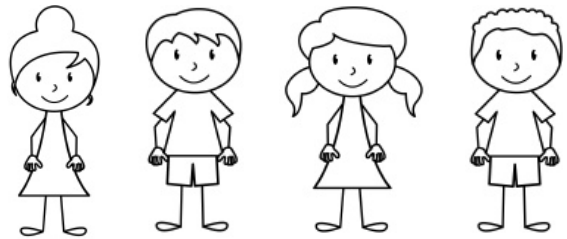
Comparaison:

Schemes	Sig. size	Ad-hoc	Times	Trac.	Full trac.
Ring signature	$O(n)$	Yes	∞	-	-
Short group sig.	$O(1)$	No	∞	-	-
Linkable sig.	$O(n)$	Yes	1	No	-
List sig. (Ad-hoc)	$O(n)$	Yes	1	Yes	-
k-times group sig.	$O(1)$	No	k	Yes	No
Ktrace	$\mathbf{O(n \cdot k)}$	**Yes**	k	**Yes**	**Yes**

Future works:

- Short signature size
- Full traceable group signatures
- Without random oracle
- Without pairing

Thank you for your attention!



questions?