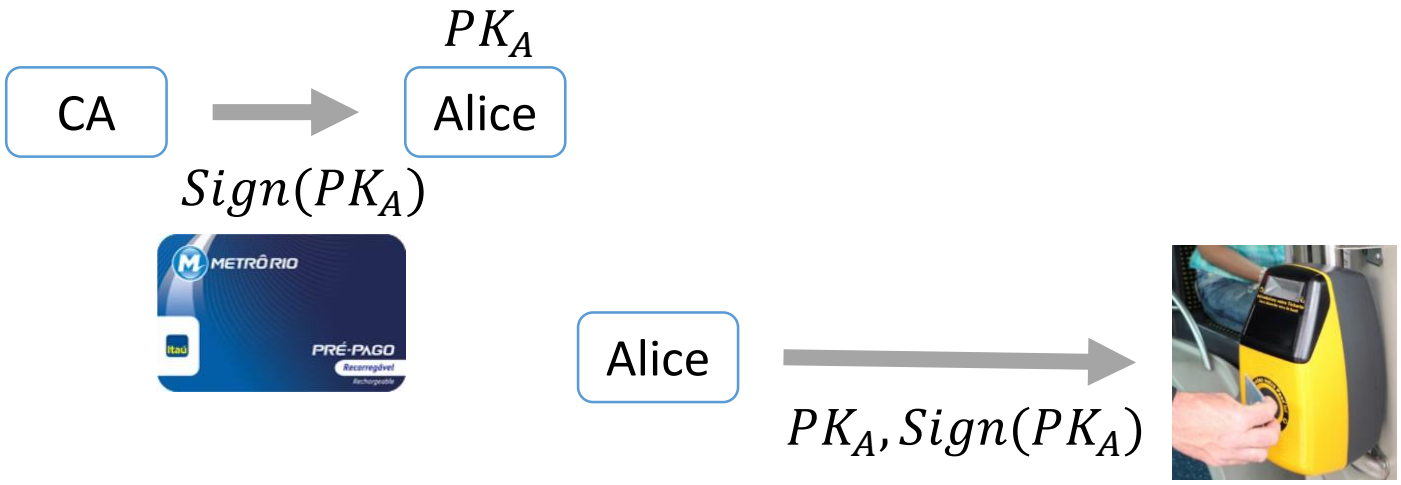
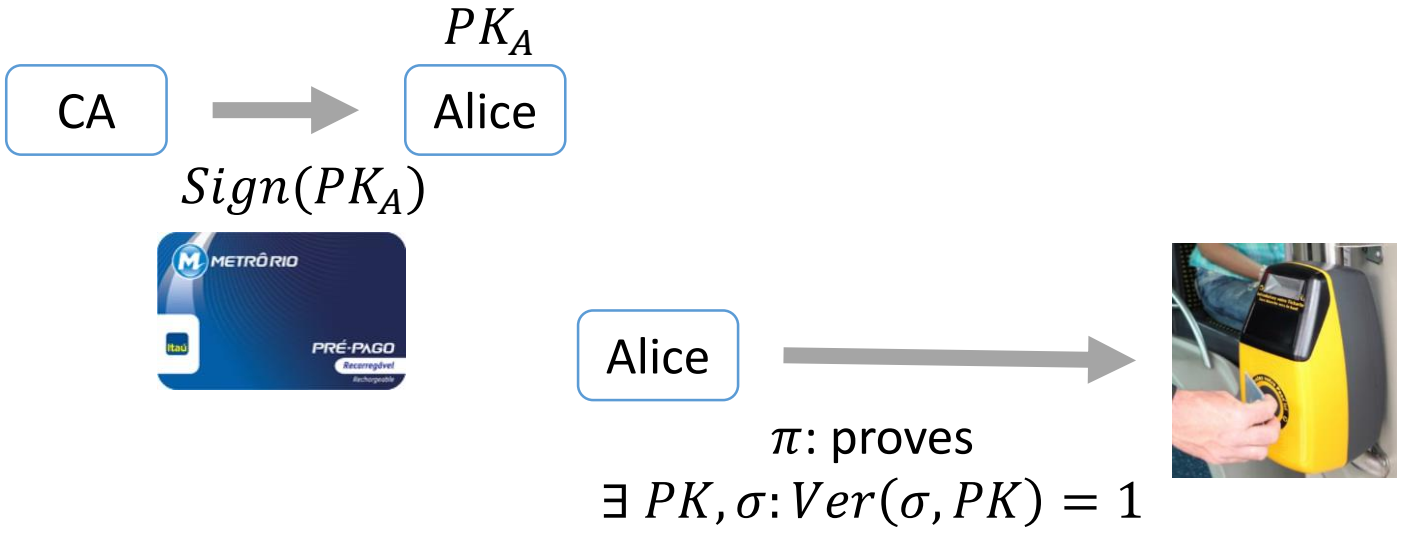
Weakly Secure Equivalence-Class Signatures from Standard Assumptions

Romain Gay ……..ENS
Georg Fuchsbauer … ENS & Inria

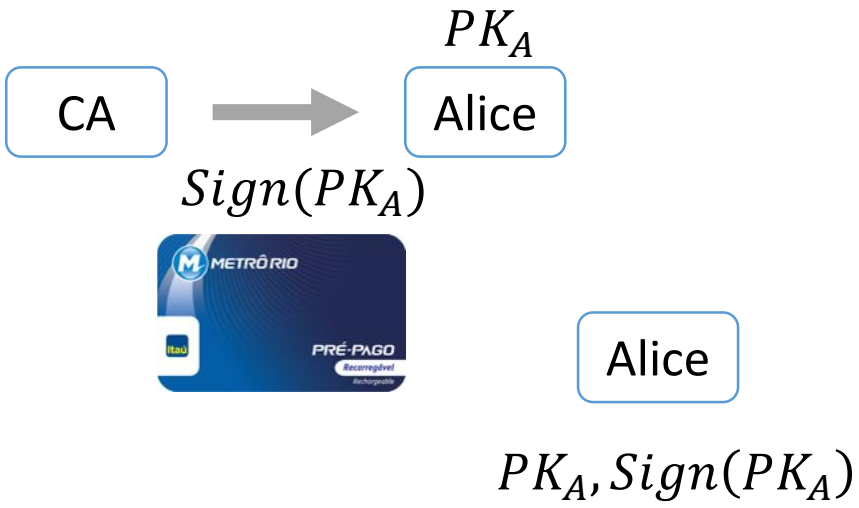
Motivation: Anonymous Credentials



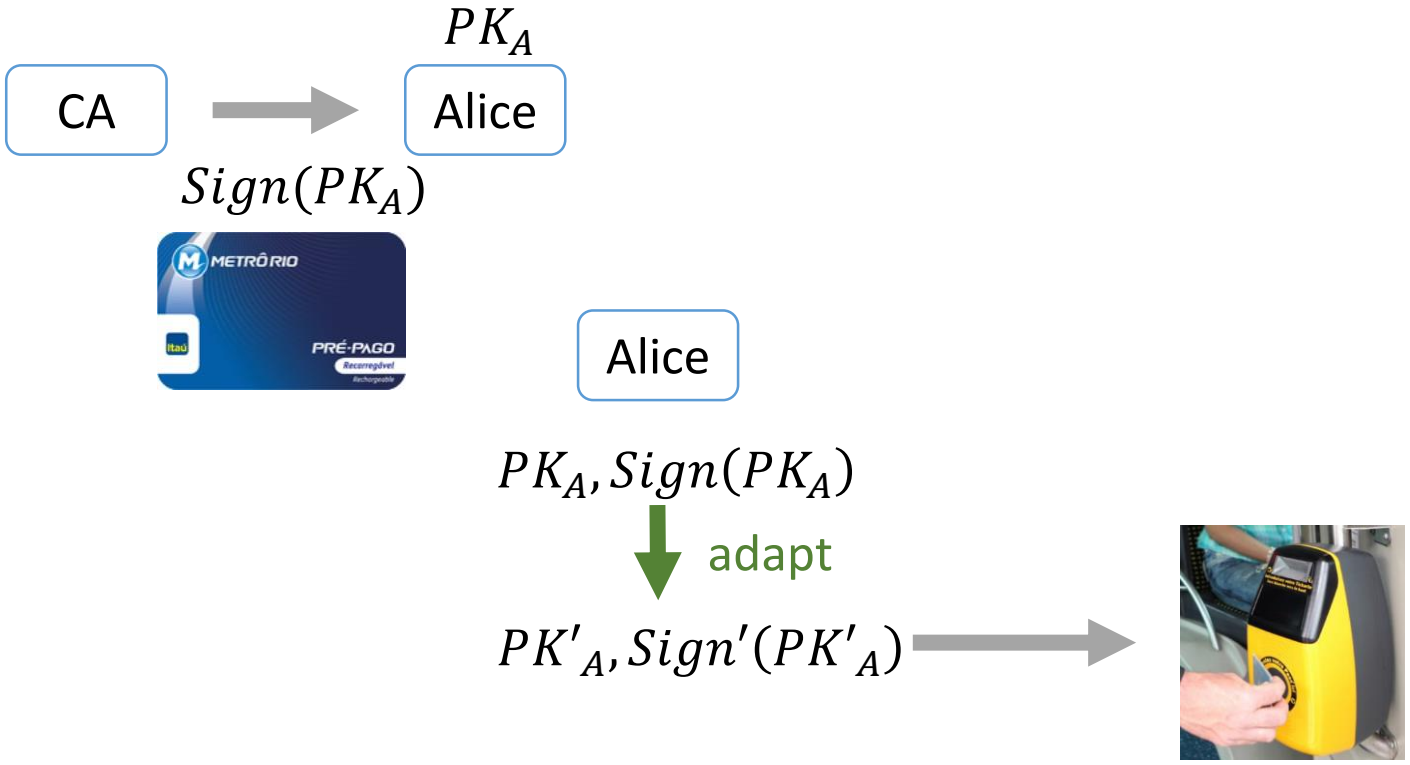
Motivation: Anonymous Credentials



Motivation: Anonymous Credentials



Motivation: Anonymous Credentials



Motivation: Anonymous Credentials

$PK_A = (g, g^a)$

CA → Alice

$Sign(PK_A)$

Alice

$(g, g^a), Sign(g, g^a)$

$r \leftarrow \mathbb{Z}_p$

$(g^r, g^{ra}), Sign(g^r, g^{ra})$ →

Equivalence Class Signatures

[Fuchsbauer, Hanser, Slamanig 14]

- $Setup(1^\lambda, \mathbb{G}): sk, pk$
- $Sign(sk, M \in \mathbb{G}^\ell): \sigma$
- $Adapt(pk, \sigma, r \in \mathbb{Z}_p^*): \sigma'$
- $Ver(pk, M, \sigma)$: bit

Equivalence Class Signatures

[Fuchsbauer, Hanser, Slamanig 14]

- $Setup(1^\lambda, \mathbb{G})$: sk, pk
- $Sign(sk, M \in \mathbb{G}^\ell)$: σ
- $Adapt(pk, \sigma, r \in \mathbb{Z}_p^*)$: σ'
- $Ver(pk, M, \sigma)$: bit

Adaptation:

$$\forall M \in \mathbb{G}^\ell, \forall r \in \mathbb{Z}_p^* :$$
$$Adapt(pk, Sign(sk, M), r) \approx Sign(sk, M^r)$$

Equivalence Class Signatures

[Fuchsbauer, Hanser, Slamanig 14]

- $Setup(1^\lambda, \mathbb{G}): sk, pk$
- $Sign(sk, M \in \mathbb{G}^\ell): \sigma$
- $Adapt(pk, \sigma, r \in \mathbb{Z}_p^*): \sigma'$
- $Ver(pk, M, \sigma)$: bit

Adaptation:

$$\forall M \in \mathbb{G}^\ell, \forall r \in \mathbb{Z}_p^* :$$
$$Adapt(pk, Sign(sk, M), r) \approx Sign(sk, M^r)$$

For any $M = (g_1, \dots, g_\ell)$, $\quad M^r = (g_1^r, \dots, g_\ell^r)$

Equivalence Class Signatures

[Fuchsbauer, Hanser, Slamanig 14]

- $Setup(1^\lambda, \mathbb{G}): sk, pk$
- $Sign(sk, M \in \mathbb{G}^\ell): \sigma$
- $Adapt$
- $Ver(p$

Many applications:

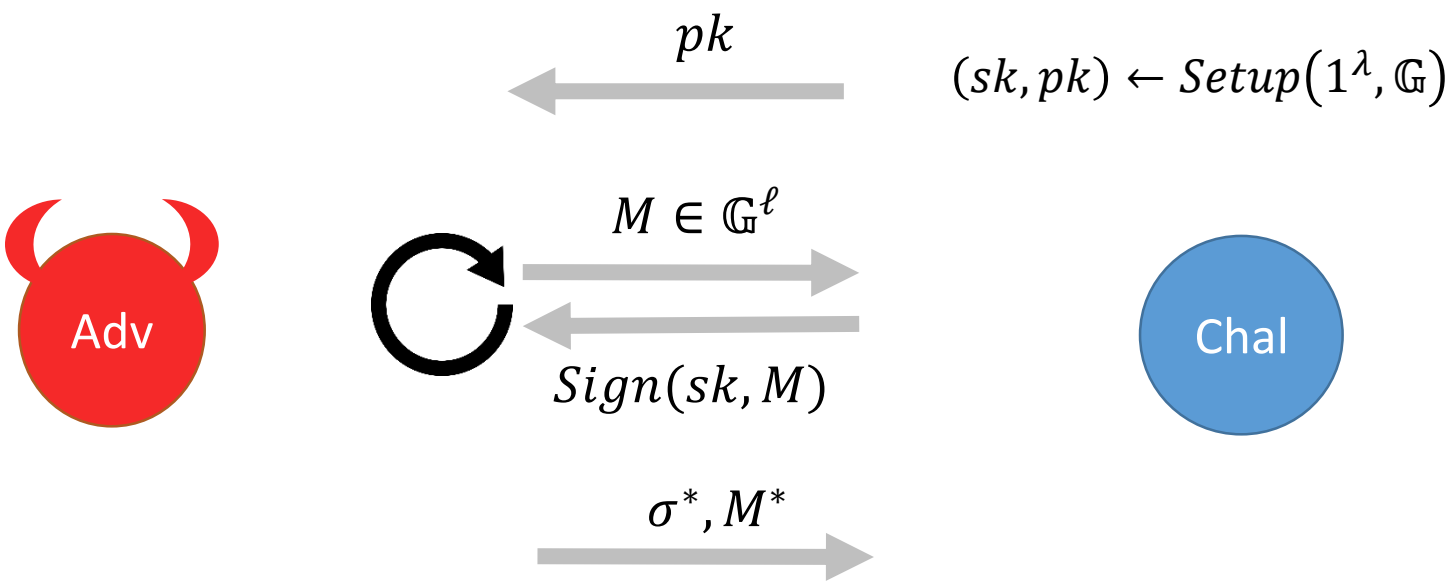
- Anonymous Credentials [FHS 14, DHS 15]
- Blind Signatures [FHS 15, FHKS 16]
- Access Control Encryption [FGKO 17]
- Group Signatures [DS 16]

$$\forall M \in \mathbb{G}^\ell, \forall r \in \mathbb{Z}_p^* :$$
$$Adapt(pk, Sign(sk, M), r) \approx Sign(sk, M^r)$$

For any $M = (g_1, \dots, g_\ell)$, $\quad M^r = (g_1^r, \dots, g_\ell^r)$

Equivalence Class Signatures

[Fuchsbauer, Hanser, Slamanig 14]

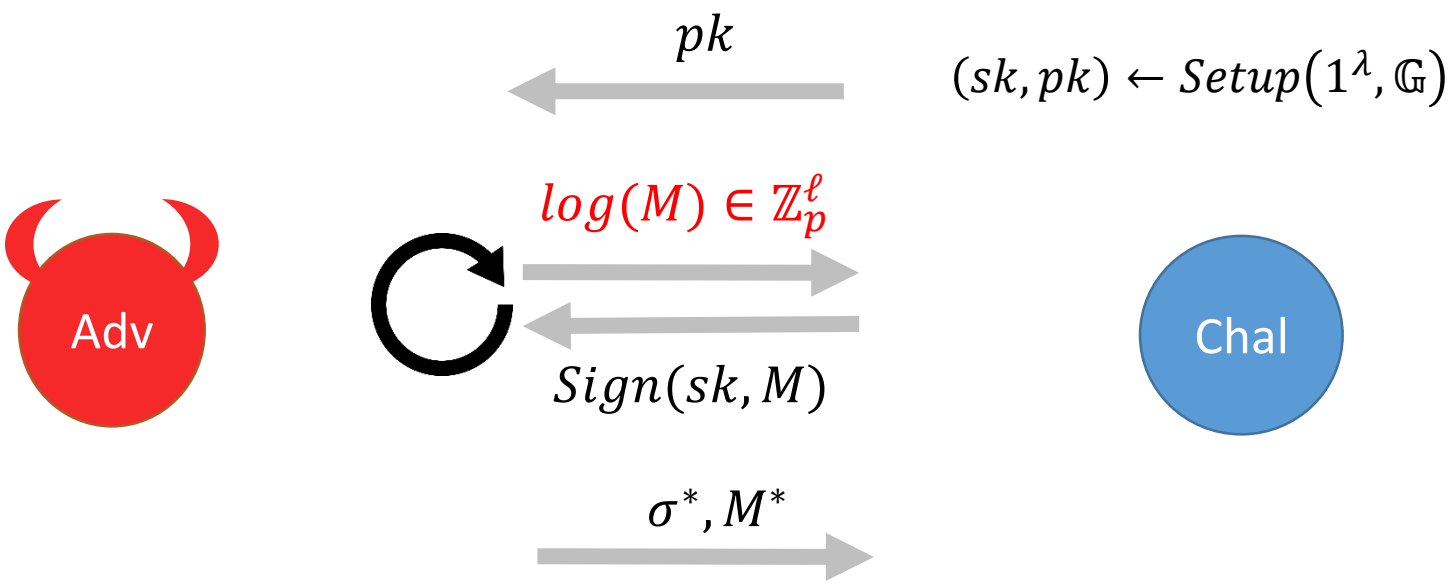


Win:

$Ver(pk, M^*, \sigma^*)$ and M^* not multiple of any queried M

Equivalence Class Signatures

[Fuchsbauer, Hanser, Slamanig 14]



Win:

$Ver(pk, M^*, \sigma^*)$ and M^* not multiple of any queried M

Our Result

Construction:	Unforgeability:	Assumption:
[HS 14]	Random-message	GGM
[FHS 14]	EUF-CMA	GGM
ours	Weak EUF-CMA	DLIN

Many applications:

- Anonymous Credentials [FHS 14, DHS 15]
- Blind Signatures [FHS 15, FHKS 16]
- Access Control Encryption [FGKO 17]
- Group Signatures [DS 16]

Outline

1. MAC on Equivalence Classes:
one-time, statistical

2. MAC on Equivalence Classes:
Many-time, pairing-based

[KW 15]

3. Signature on Equivalence Classes
Many-time, pairing-based

Outline

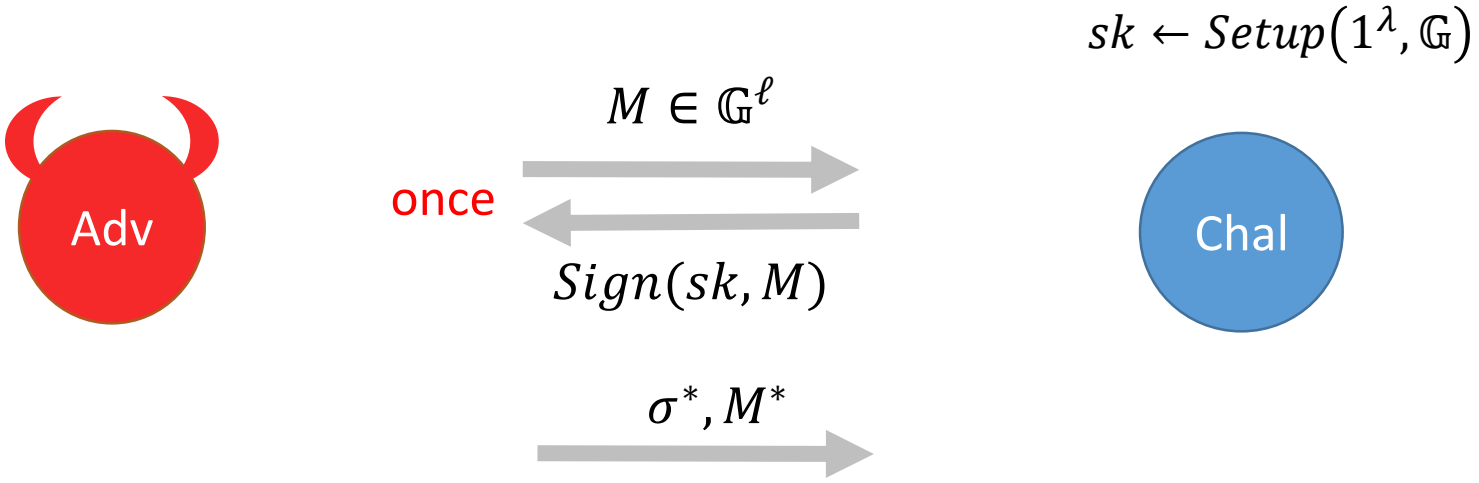
1. MAC on Equivalence Classes:
one-time, statistical

2. MAC on Equivalence Classes:
Many-time, pairing-based

[KW 15]

3. Signature on Equivalence Classes
Many-time, pairing-based

One-time MAC on Equivalence Classes



Win:

$Ver(sk, M^*, \sigma^*)$ and M^* not multiple of the queried M

One-time MAC on Equivalence Classes

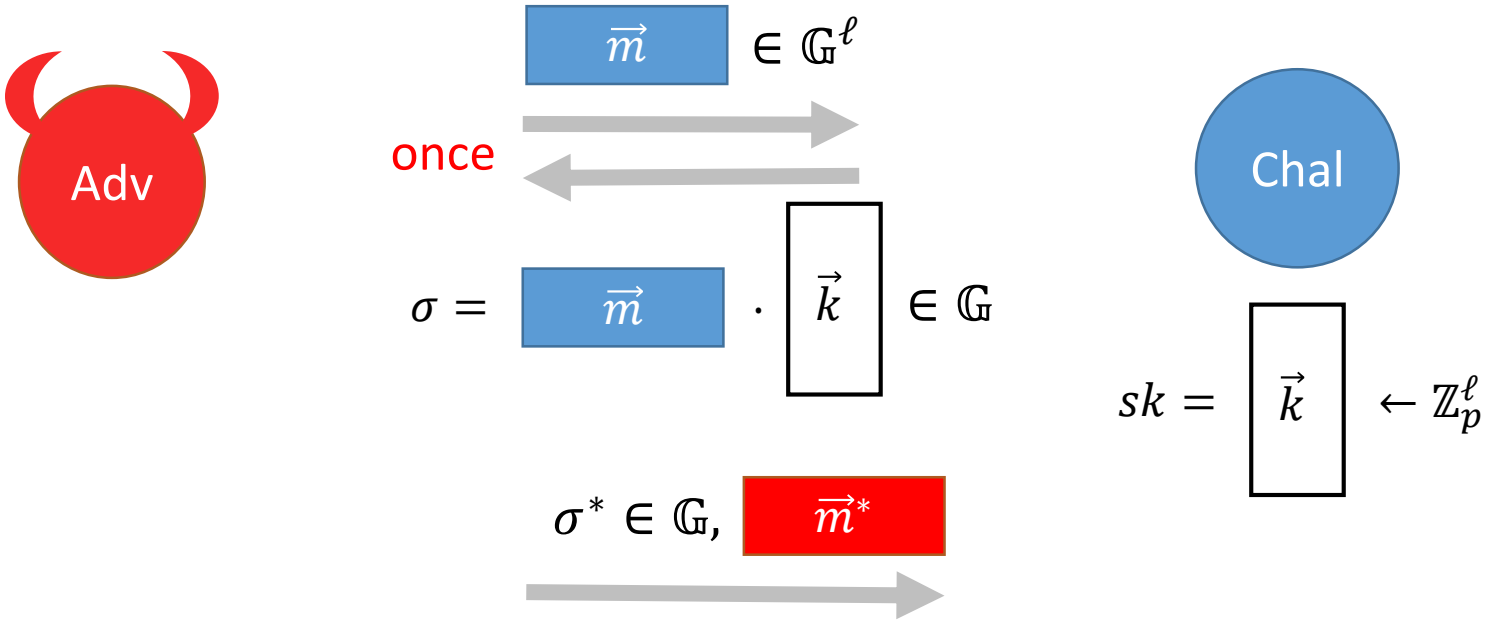
$\mathbb{G}$ of order p, generator g

$$sk = \boxed{\vec{k}} \leftarrow \mathbb{Z}_p^{\ell}$$

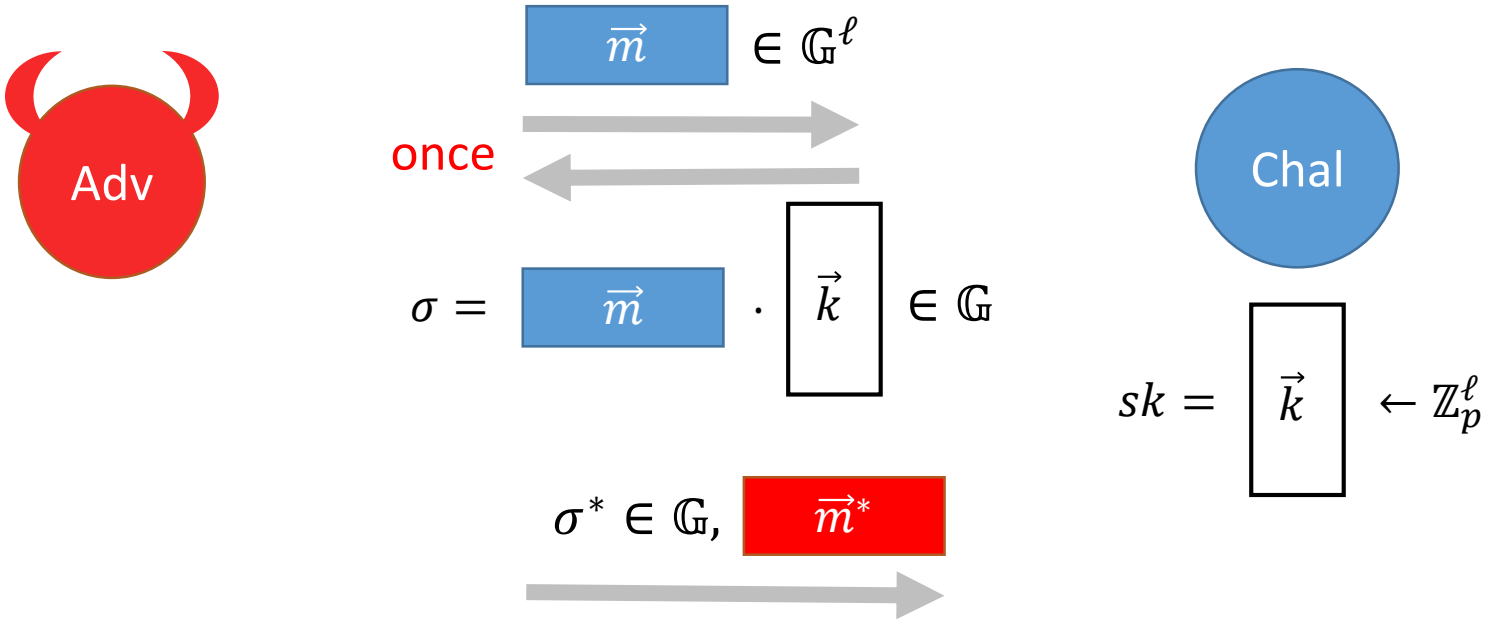
$$Sign(sk, \boxed{\vec{m}} = g^{\vec{m}} \in \mathbb{G}^{\ell}): \boxed{\vec{m}} \cdot \boxed{\vec{k}} = g^{\vec{m}\cdot\vec{k}} \in \mathbb{G}$$

$$Adapt\left(\sigma \in \mathbb{G}, r \in \mathbb{Z}_p^*\right): \sigma^r$$

One-time MAC on Equivalence Classes



One-time MAC on Equivalence Classes

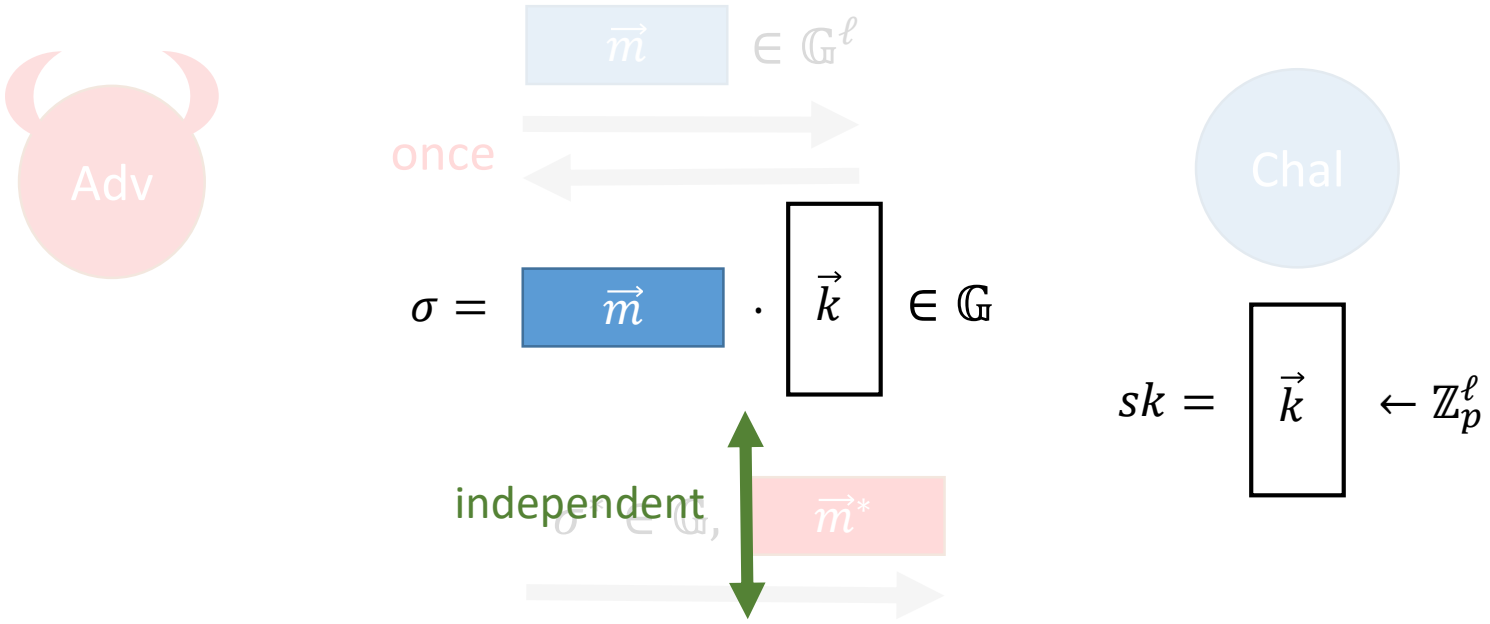


Win:

$\sigma^* = \vec{m}^* \cdot \vec{k}$

and $\vec{m}^*$ not multiple of $\vec{m}$

One-time MAC on Equivalence Classes



Win:

$\sigma^* = \vec{m}^* \cdot \vec{k}$

and $\vec{m}^*$ not multiple of $\vec{m}$

Outline

1. MAC on Equivalence Classes:
one-time, statistical

2. MAC on Equivalence Classes:
Many-time, pairing-based

[KW 15]

3. Signature on Equivalence Classes
Many-time, pairing-based

MAC on Equivalence Classes

$e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ of order p, generators $g_1, g_2, g_T = e(g_1, g_2)$

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

MAC on Equivalence Classes

$e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ of order p, generators $g_1, g_2, g_T = e(g_1, g_2)$

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

$\vec{a} \leftarrow \mathbb{G}_2^2$, $\vec{a}r$ with $r \leftarrow \mathbb{Z}_p$ $\approx_{DDH}$ $\vec{a} \leftarrow \mathbb{G}_2^2$, $\vec{u} \leftarrow \mathbb{G}_2^2$

MAC on Equivalence Classes

$e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ of order p, generators $g_1, g_2, g_T = e(g_1, g_2)$

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

$\vec{a} \leftarrow \mathbb{G}_2^2$, $\vec{a}r$ with $r \leftarrow \mathbb{Z}_p$ $\approx_{DDH}$ $\vec{a} \leftarrow \mathbb{G}_2^2$, $\vec{u} \leftarrow \mathbb{G}_2^2$

$K \leftarrow \mathbb{Z}_p^{\ell \times 2}$ $K \cdot \vec{a}r$ independent $K \cdot \vec{u}$

MAC on Equivalence Classes

$e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ of order p, generators $g_1, g_2, g_T = e(g_1, g_2)$

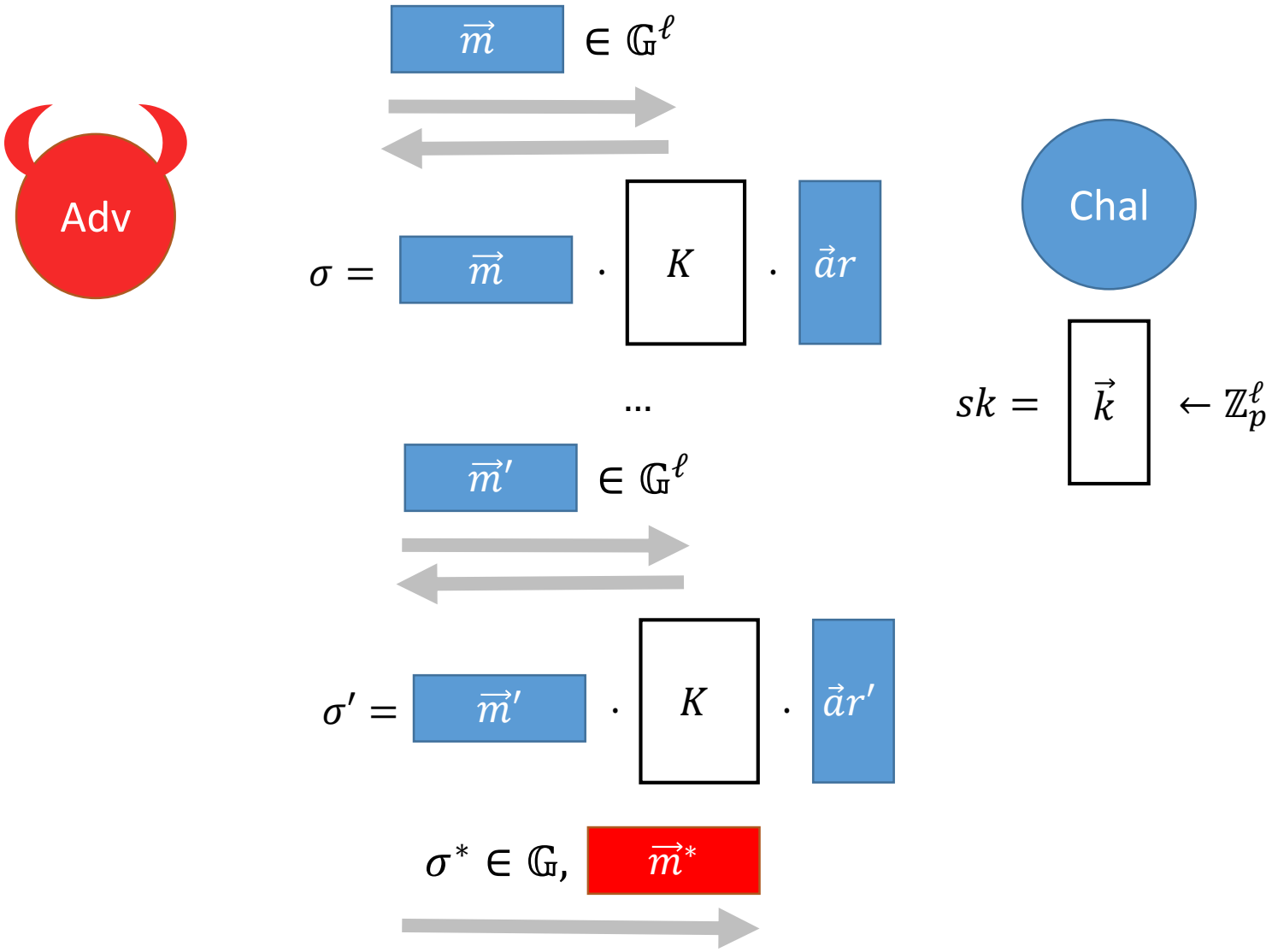
$sk =$ K $\leftarrow \mathbb{Z}_p^{\ell \times 2}$, $\vec{a}$ $\leftarrow \mathbb{G}_2^2$

$Sign(sk,$ $\vec{m}$ $= g_1^{\vec{m}} \in \mathbb{G}_1^{\ell})$: $\vec{m}$ $\cdot$ K $\cdot$ $\vec{a}r$ $= e(g_1, g_2)^{\vec{m} \cdot K \cdot \vec{a}r} \in \mathbb{G}_T$

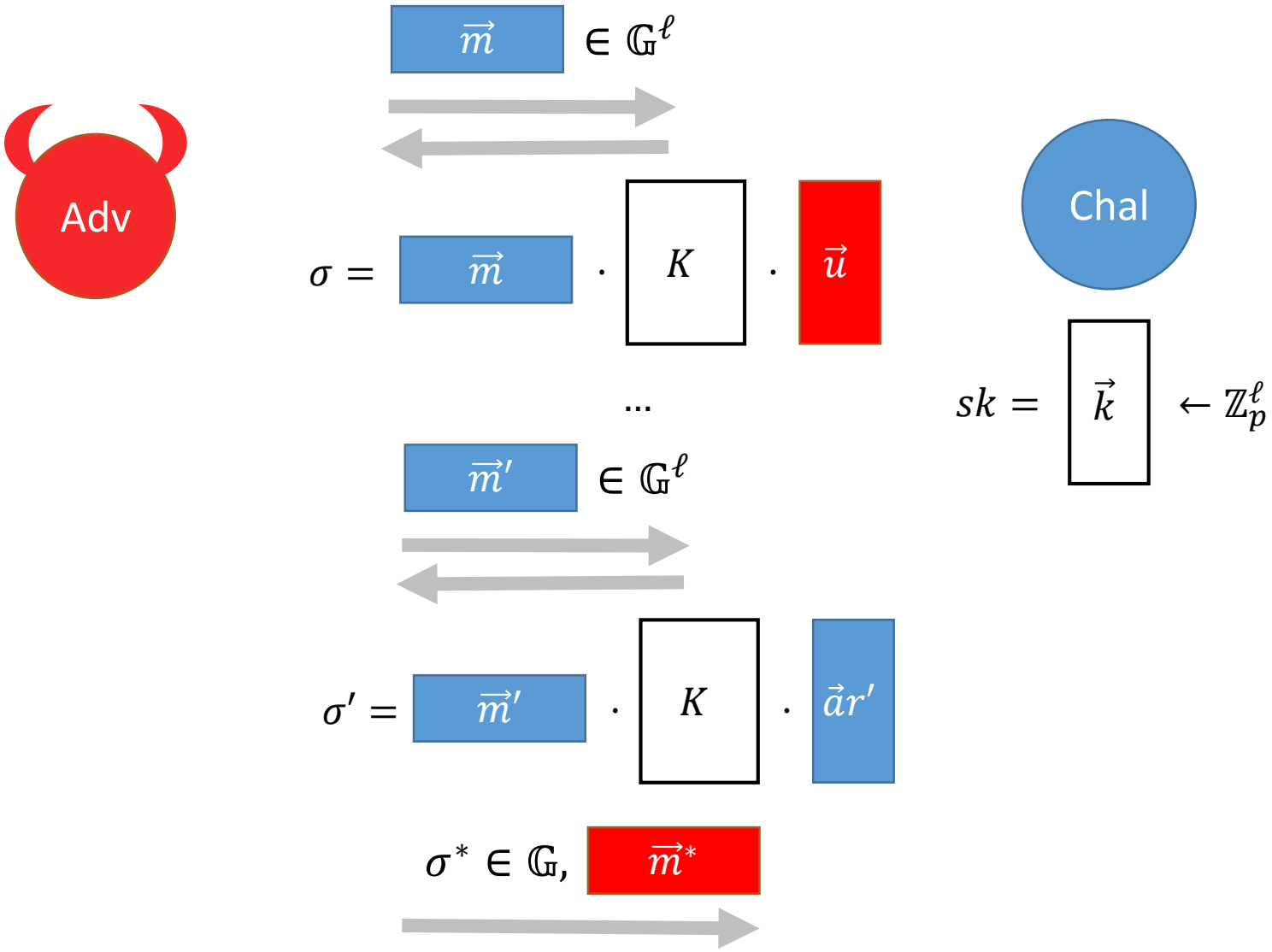
$r \leftarrow \mathbb{Z}_p$

$\vec{a}r$ $\in \mathbb{G}_2^2$

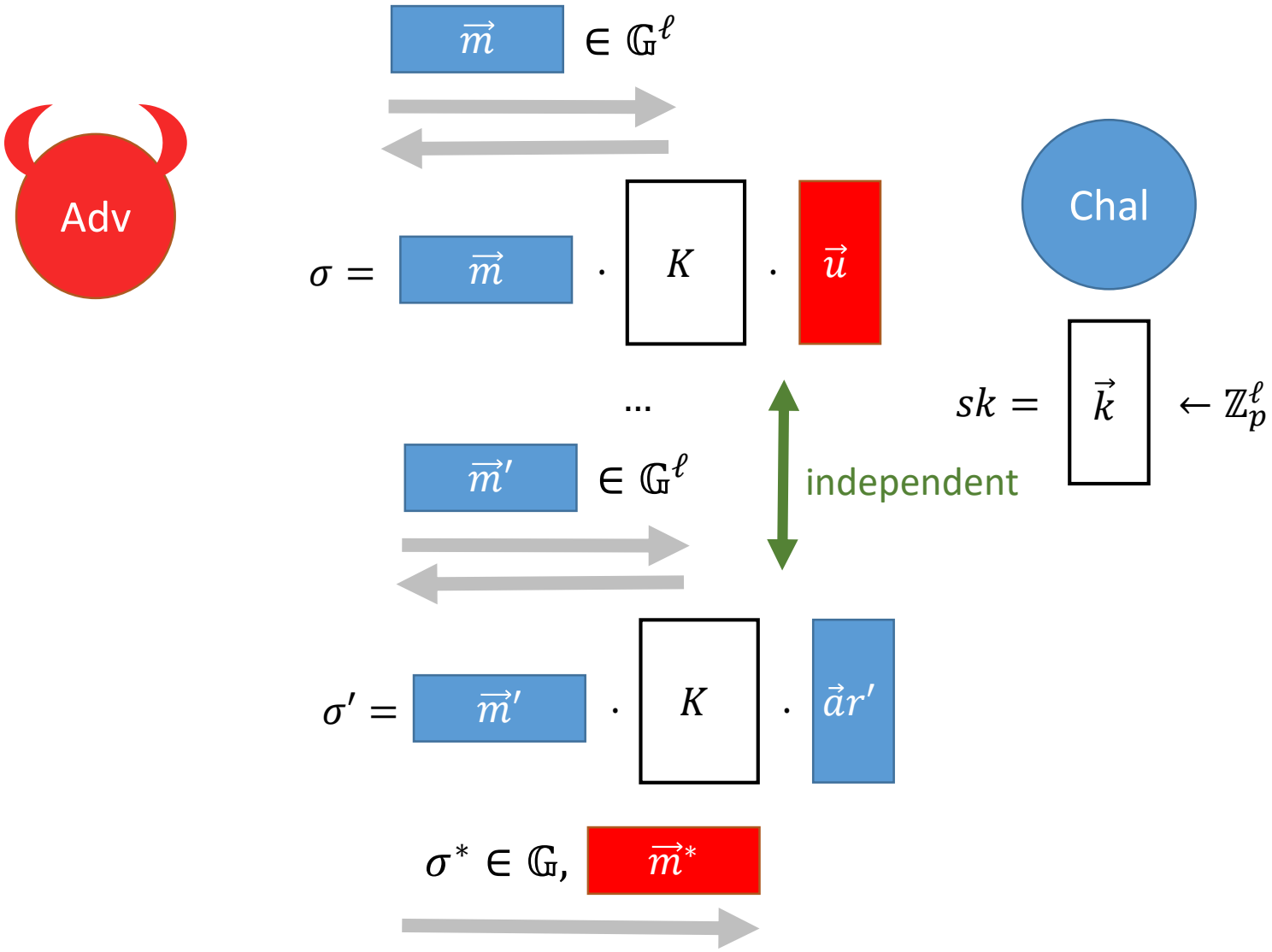
MAC on Equivalence Classes



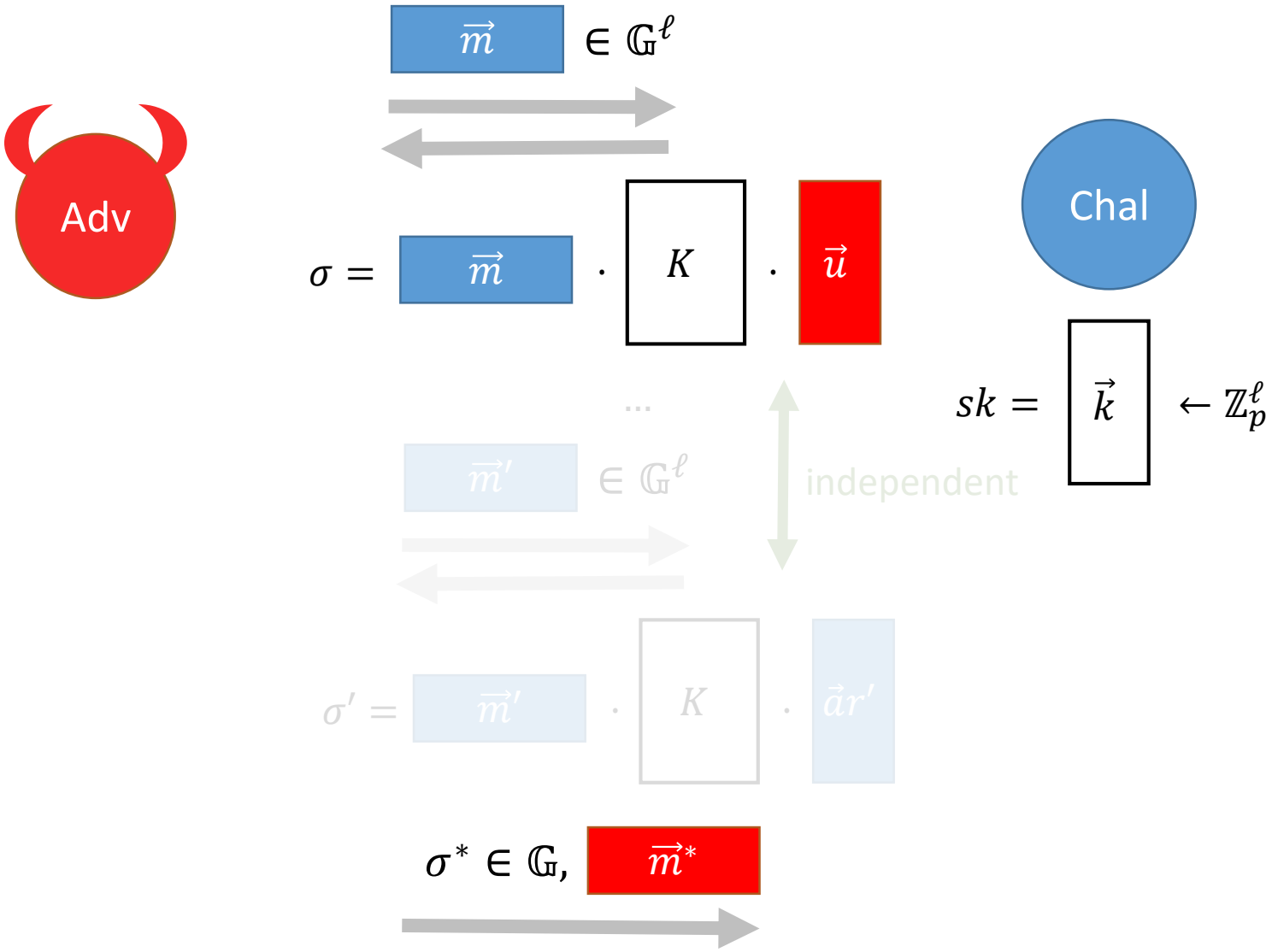
MAC on Equivalence Classes



MAC on Equivalence Classes



MAC on Equivalence Classes



Outline

1. MAC on Equivalence Classes:
one-time, statistical

2. MAC on Equivalence Classes:
Many-time, pairing-based

[KW 15]

3. Signature on Equivalence Classes
Many-time, pairing-based

MAC on Equivalence Classes

$e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ of order p, generators $g_1, g_2, g_T = e(g_1, g_2)$

$sk = K \leftarrow \mathbb{Z}_p^{\ell \times 2}$, $\vec{a} \leftarrow \mathbb{G}_2^2$

$Sign(sk, \vec{m} = g_1^{\vec{m}} \in \mathbb{G}_1^{\ell})$: $\vec{m} \cdot K \cdot \vec{a}r$, $\vec{a}r \in \mathbb{G}_2^2$

$r \leftarrow \mathbb{Z}_p$

$= e(g_1, g_2)^{\vec{m} \cdot K \cdot \vec{a}r} \in \mathbb{G}_T$

MAC on Equivalence Classes

$\mathbb{G}$ of order p, generators g

$sk =$ K $\leftarrow \mathbb{Z}_p^{\ell \times 2}$, $\vec{a}$ $\leftarrow \mathbb{G}^2$

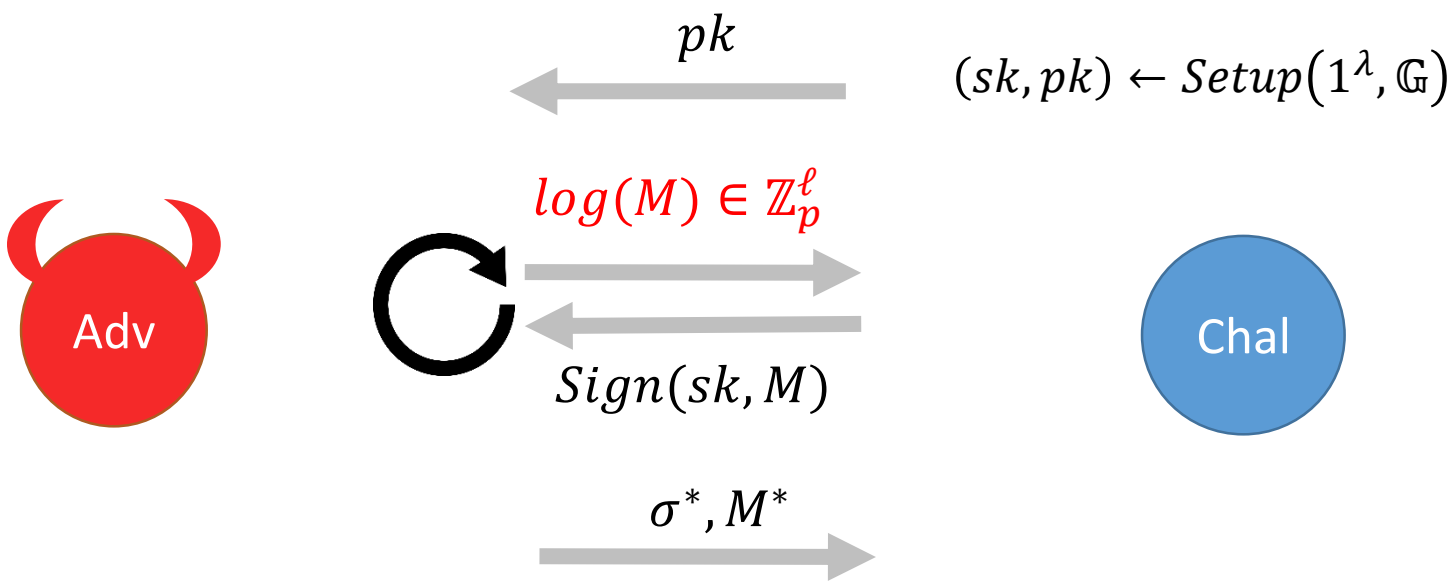
$Sign(sk,$ $\vec{m}$ $\in \mathbb{Z}_p^{\ell})$:

$r \leftarrow \mathbb{Z}_p$

$\vec{m}$ $\cdot$ K $\cdot$ $\vec{a}r$, $\vec{a}r$ $\in \mathbb{G}^2$

$= g^{\vec{m} \cdot K \cdot \vec{a}r} \in \mathbb{G}$

Equivalence Class Signatures (EQS)



Win:

$Ver(pk, M^*, \sigma^*)$ and M^* not multiple of any queried M

Equivalence Class Signatures

- $Setup\left(1^{\lambda}, \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T\right): sk, pk$
- $Sign(sk, \boxed{\vec{m}} = g_1^{\vec{m}} \in \mathbb{G}_1^{\ell}): \sigma$
- $Adapt\left(pk, \sigma, r \in \mathbb{Z}_p^*\right): \sigma'$
- $Ver(pk, M, \sigma)$: bit

Equivalence Class Signatures

- $Setup\left(1^{\lambda}, \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T\right): sk, pk$
- $Sign(sk, \boxed{\vec{m}} = g_1^{\vec{m}} \in \mathbb{G}_1^{\ell}): \sigma$
- $Adapt\left(pk, \sigma, r \in \mathbb{Z}_p^*\right): \sigma' \in \mathbb{G}_1^{4\ell+2} \times \mathbb{G}_2^4$
- $Ver(pk, M, \sigma)$: bit

Conclusion

Construction:	Unforgeability:	Assumption:	Sign. Size:
[FHS 14]	EUF-CMA	GGM	$2\|\mathbb{G}_1\| + \|\mathbb{G}_2\|$
ours	Weak EUF-CMA	DLIN	$(4\ell + 2)\|\mathbb{G}_1\| + 4\|\mathbb{G}_2\|$

Many applications:

- Anonymous Credentials [FHS 14, DHS 15]
- Blind Signatures [FHS 15, FHKS 16]
- Access Control Encryption [FGKO 17]
- Group Signatures [DS 16]

Conclusion

Construction:	Unforgeability:	Assumption:	Sign. Size:
[FHS 14]	EUF-CMA	GGM	$2\|\mathbb{G}_1\| + \|\mathbb{G}_2\|$
ours	Weak EUF-CMA	DLIN	$(4\ell + 2)\|\mathbb{G}_1\| + 4\|\mathbb{G}_2\|$

Thank you

Many applications:

- Anonymous Credentials [FHS 14, DHS 15]
- Blind Signatures [FHS 15, FHKS 16]
- Access Control Encryption [FGKO 17]
- Group Signatures [DS 16]