## Access Control Encryption for Equality, Comparison, and More

Georg Fuchsbauer, ENS
Romain Gay, ENS

PSL太
CINVENTORS FORTHEDIIITALWORLD

Lucas Kowalczyk, Columbia University
Claudio Orlandi, Aarhus university

European
Research Council

## ACE [Damgård, Haagh, Orlandi 16]

Senders:


Receivers:



## ACE [Damgård, Haagh, Orlandi 16]

Senders:


Receivers:

secret


## ACE [Damgård, Haagh, Orlandi 16]

Senders: $\mathrm{ek}_{1}, \mathrm{ek}_{2}, \mathrm{ek}_{3}$ Trusted setup $\mathrm{dk}_{1}, \mathrm{dk}_{2}, \mathrm{dk}_{3}$


## ACE [Damgård, Haagh, Orlandi 16]


top-secret

$\mathrm{ek}_{1}$


## ACE [Damgård, Haagh, Orlandi 16]


top-secret

$\mathrm{ek}_{3}$
public
$\mathrm{ek}_{1}$


## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## ACE [Damgård, Haagh, Orlandi 16]



## Previous works

$$
\text { For predicates } P:\{0,1\}^{\mathrm{n}} \times\{0,1\}^{\mathrm{n}} \rightarrow\{0,1\}
$$

| Construction: | Predicate: | Ct size: | Assumption: | Practical: |
| :--- | :---: | :---: | :---: | :---: |
| [DHO 16] | any | $O\left(2^{n}\right)$ | DDH or DCR | (DO |
| [DHO 16] | any | $\operatorname{poly}(n)$ | iO | $\$$ |

## Our work

For predicates P: $\{0,1\}^{\mathrm{n}} \times\{0,1\}^{\mathrm{n}} \rightarrow\{0,1\}$

| Construction: | Predicate: | Ct size: | Assumption: | Practical: |
| :--- | :---: | :---: | :---: | :---: |
| [DHO 16] | any | $O\left(2^{n}\right)$ | DDH or DCR |  |
| [DHO 16] | any | poly $(n)$ | iO | - |
| Our work | $\mathrm{P}_{\text {eq }}, \mathrm{P}_{\text {comp }}$ | $O(n)$ | SXDH |  |

$$
\begin{aligned}
& P_{e q}(i, j)=1 \text { iff } i=j \\
& P_{\text {comp }}(i, j)=1 \text { iff } i \geq j
\end{aligned}
$$

## Outline



1. ACE for equality from [DHO 16]
2. New ACE for equality

## ACE for equality: DHO 16



## ACE for equality: DHO 16

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Private Key Encryption

Senders:


$$
\mathrm{ek}_{1}, \mathrm{ek}_{2}, \mathrm{ek}_{3} \text { Trusted setup } \mathrm{dk}_{1}, \mathrm{dk}_{2}, \mathrm{dk}_{3}
$$

$\mathrm{ek}_{1}$



No-Read rule


## ACE for equality: DHO 16

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Private Key Encryption

Senders:

$\mathrm{ek}_{2}$

$$
\mathrm{ek}_{1}, \mathrm{ek}_{2}, \mathrm{ek}_{3} \text { Trusted setup } \mathrm{dk}_{1}, \mathrm{dk}_{2}, \mathrm{dk}_{3}
$$

Receivers:
$\mathrm{ek}_{1}$

$\mathrm{ek}_{3}$
$S_{3}$

## ACE for equality: DHO 16

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Public Key Encryption

Senders:

$\mathrm{ek}_{1}, \mathrm{ek}_{2}, \mathrm{ek}_{3}$ Trusted setup $\mathrm{dk}_{1}, \mathrm{dk}_{2}, \mathrm{dk}_{3}$

Receivers:


No-Read rule

$\mathrm{dk}_{3}$

## ACE for equality: DHO 16

$$
\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow \text { Anonymous Public Key Encryption }
$$

Senders:

 $\mathrm{dk}_{1}, \mathrm{dk}_{2}, \mathrm{dk}_{3}$

Receivers:

## ACE for equality: DHO 16

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Sanitizable Anonymous Public Key Encryption

Senders:

$\square$ $\mathrm{ek}_{3}$ $\mathrm{S}_{3}$


Receivers:

$\mathrm{dk}_{2}$
$\mathrm{dk}_{3}$
$\mathrm{dk}_{1}$

## ACE for equality: DHO 16

$\left(\mathrm{pk}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Sanitizable Anonymous Public Key Encryption


## ACE for equality: DHO 16

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Sanitizable Anonymous Public Key Encryption


## ACE for equality: DHO 16

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Sanitizable Anonymous Public Key Encryption


## ACE for equality: DHO 16

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Sanitizable Anonymous Public Key Encryption


## New ACE for equality

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Anonymous PKE


## New ACE for equality

$$
\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow \text { Anonymous PKE }
$$



## New ACE for equality

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Anonymous PKE, $\quad \sigma_{\mathrm{i}}=\operatorname{Sign}\left(\mathrm{ek}_{\mathrm{i}}\right)$


## New ACE for equality

$$
\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow \text { Anonymous PKE, } \quad \sigma_{\mathrm{i}}=\operatorname{Sign}\left(e \mathrm{k}_{\mathrm{i}}\right)
$$



## New ACE for equality

$$
\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow \text { Anonymous PKE, } \quad \sigma_{\mathrm{i}}=\operatorname{Sign}\left(e \mathrm{k}_{\mathrm{i}}\right)
$$



## New ACE for equality

$$
\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow \text { Anonymous PKE, } \quad \sigma_{\mathrm{i}}=\operatorname{Sign}\left(e \mathrm{k}_{\mathrm{i}}\right)
$$



## New ACE for equality

$\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow$ Anonymous PKE, $\sigma_{\mathrm{i}}=\operatorname{Sign}\left(\mathrm{ek}_{\mathrm{i}}\right), \mathrm{CRS} \leftarrow \mathrm{NIZK}$


## Concrete ACE for equality

- $\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow($ Rerandomizable)Anonymous PKE: El Gamal
- NIZK: Groth Sahai [GS 12]
- $\sigma_{\mathrm{i}}=\operatorname{Sign}\left(\mathrm{ek}_{\mathrm{i}}\right):$ Structure preserving signature

| SPS: | ek $_{\mathrm{i}}:$ | ct: | Assumption: |
| :--- | :---: | :---: | :---: |
| [KPW 12] | $7 \mathbb{G}_{1}+1 \mathbb{G}_{2}$ | $34 \mathbb{G}_{1}+16 \mathbb{G}_{2}$ | SXDH |
| [AGHO 11] | $3 \mathbb{G}_{1}+1 \mathbb{G}_{2}$ | $20 \mathbb{G}_{1}+14 \mathbb{G}_{2}$ | GGM |

## Concrete ACE for equality

- $\left(\mathrm{ek}_{\mathrm{i}}, \mathrm{dk}_{\mathrm{i}}\right) \leftarrow($ Rerandomizable)Anonymous PKE: El Gamal
- NIZK: Groth Sahai [GS 12]
- $\sigma_{\mathrm{i}}=\operatorname{Sign}\left(\mathrm{ek}_{\mathrm{i}}\right):$ Structure preserving signature

| SPS: | ek $_{\mathrm{i}}:$ | ct: | Assumption: |
| :--- | :---: | :---: | :---: |
| [KPW 12] | $7 \mathbb{G}_{1}+1 \mathbb{G}_{2}$ | $34 \mathbb{G}_{1}+16 \mathbb{G}_{2}$ | SXDH |
| [AGHO 11] | $3 \mathbb{G}_{1}+1 \mathbb{G}_{2}$ | $20 \mathbb{G}_{1}+14 \mathbb{G}_{2}$ | GGM |
| SPS-EQ: | $\mathrm{ek}_{\mathrm{i}}:$ | ct: | Assumption: |
| [FHS 15] | $3 \mathbb{G}_{1}+1 \mathbb{G}_{2}$ | $6 \mathbb{G}_{1}+1 \mathbb{G}_{2}$ | GGM |

## Conclusion

| Construction: | Predicate: | Ct size: | Assumption: | Practical: |
| :--- | :---: | :---: | :---: | :---: |
| [DHO 16] | any | $O\left(2^{n}\right)$ | DDH or DCR | - |
| [DHO 16] | any | $\operatorname{poly}(n)$ | iO | - |
| Our work | $\mathrm{P}_{\text {eq }}, \mathrm{P}_{\text {comp }}$ | $O(n)$ | SXDH |  |

## Conclusion

| Construction: | Predicate: | Ct size: | Assumption: | Practical: |
| :--- | :---: | :---: | :---: | :---: |
| [DHO 16] | any | $O\left(2^{n}\right)$ | DDH or DCR |  |
| [DHO 16] | any | poly $(n)$ | iO |  |
| Our work | $\mathrm{P}_{\text {eq }}, \mathrm{P}_{\text {comp }}$ | $O(n)$ | SXDH |  |
| Open | $\mathrm{P}_{\text {eq }}, \mathrm{P}_{\text {comp }}$ | $\operatorname{poly}(n)$ | DDH |  |

## Conclusion

| Construction: | Predicate: | Ct size: | Assumption: | Practical: |
| :--- | :---: | :---: | :---: | :---: |
| [DHO 16] | any | $O\left(2^{n}\right)$ | DDH or DCR |  |
| [DHO 16] | any | poly $(n)$ | iO |  |
| Our work | $\mathrm{P}_{\text {eq }}, \mathrm{P}_{\text {comp }}$ | $O(n)$ | SXDH |  |
| Open | $\mathrm{P}_{\text {eq }}, \mathrm{P}_{\text {comp }}$ | poly $(n)$ | DDH |  |
| Open | any | poly $(n)$ | standard |  |

Thank you!

