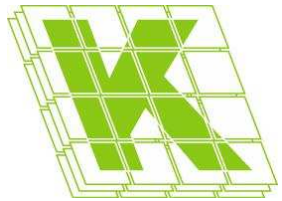
"Twenty-four"

Sebastiaan Indesteege[1] Florian Mendel[2]
Bart Preneel[1] Christian Rechberger[2]

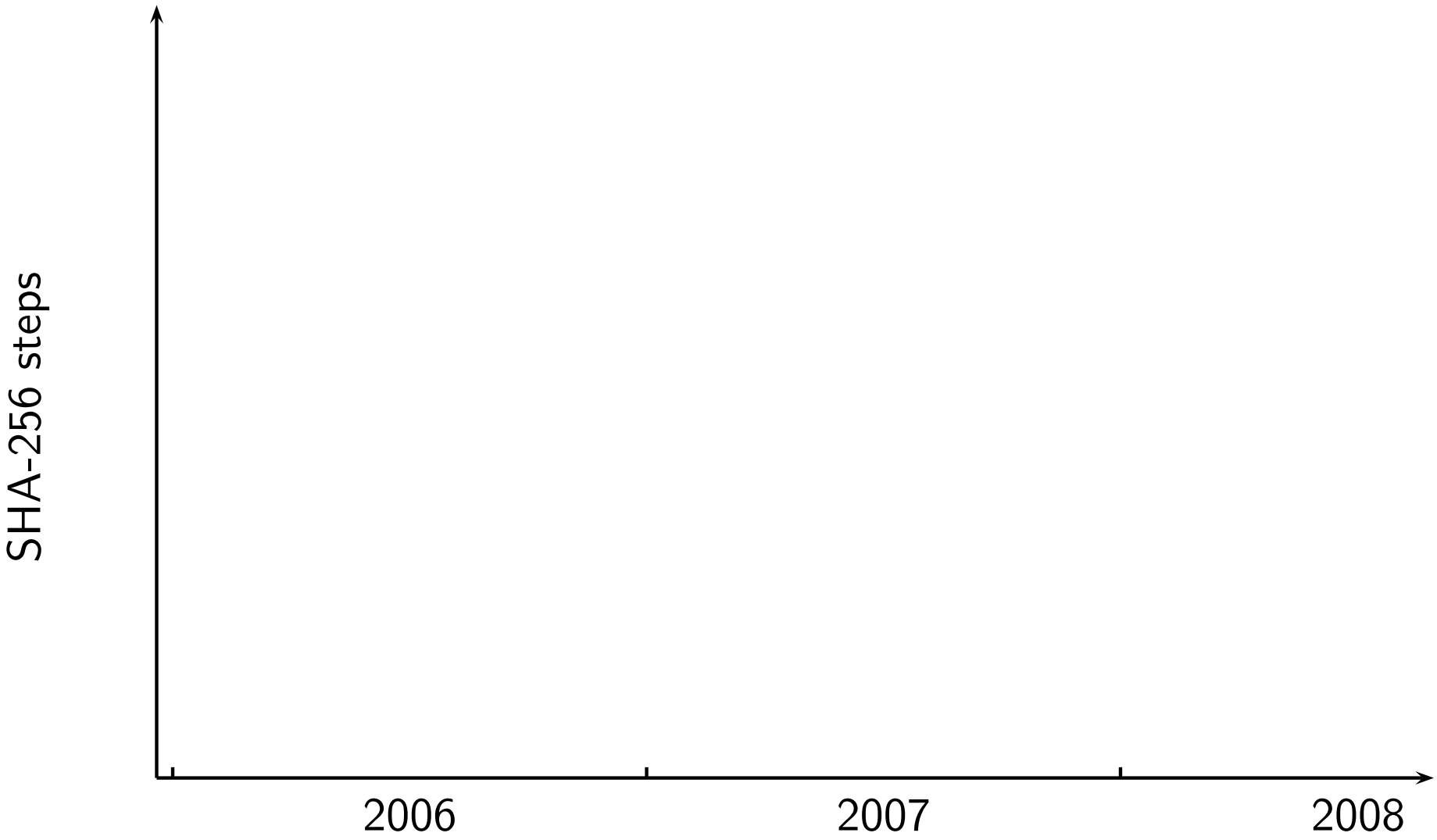
[1]COSIC, ESAT/SCD, KU Leuven, Belgium.

[2]Krypto group, IAIK, TU Graz, Austria.

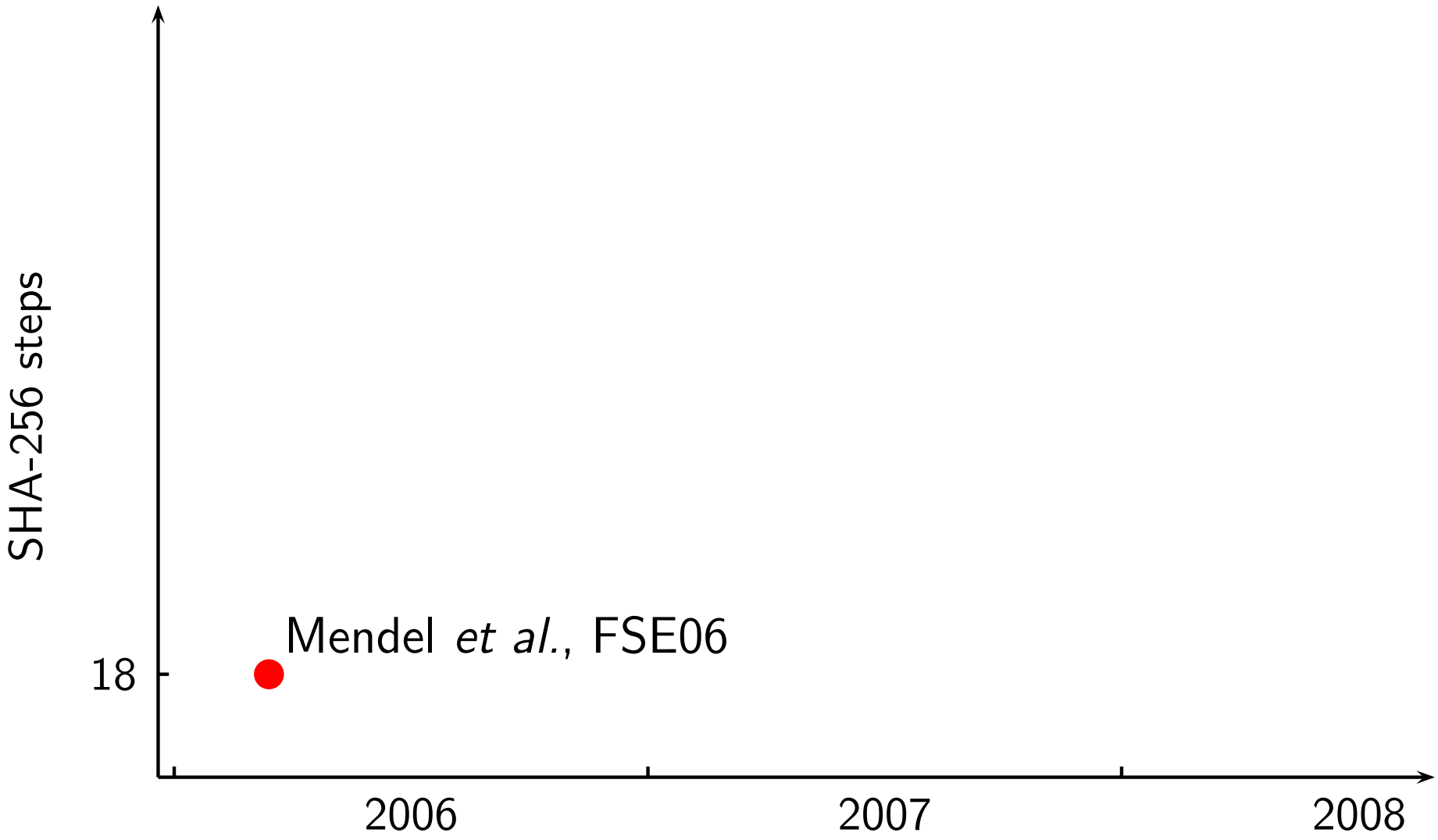
EUROCRYPT 2008 Rump Session



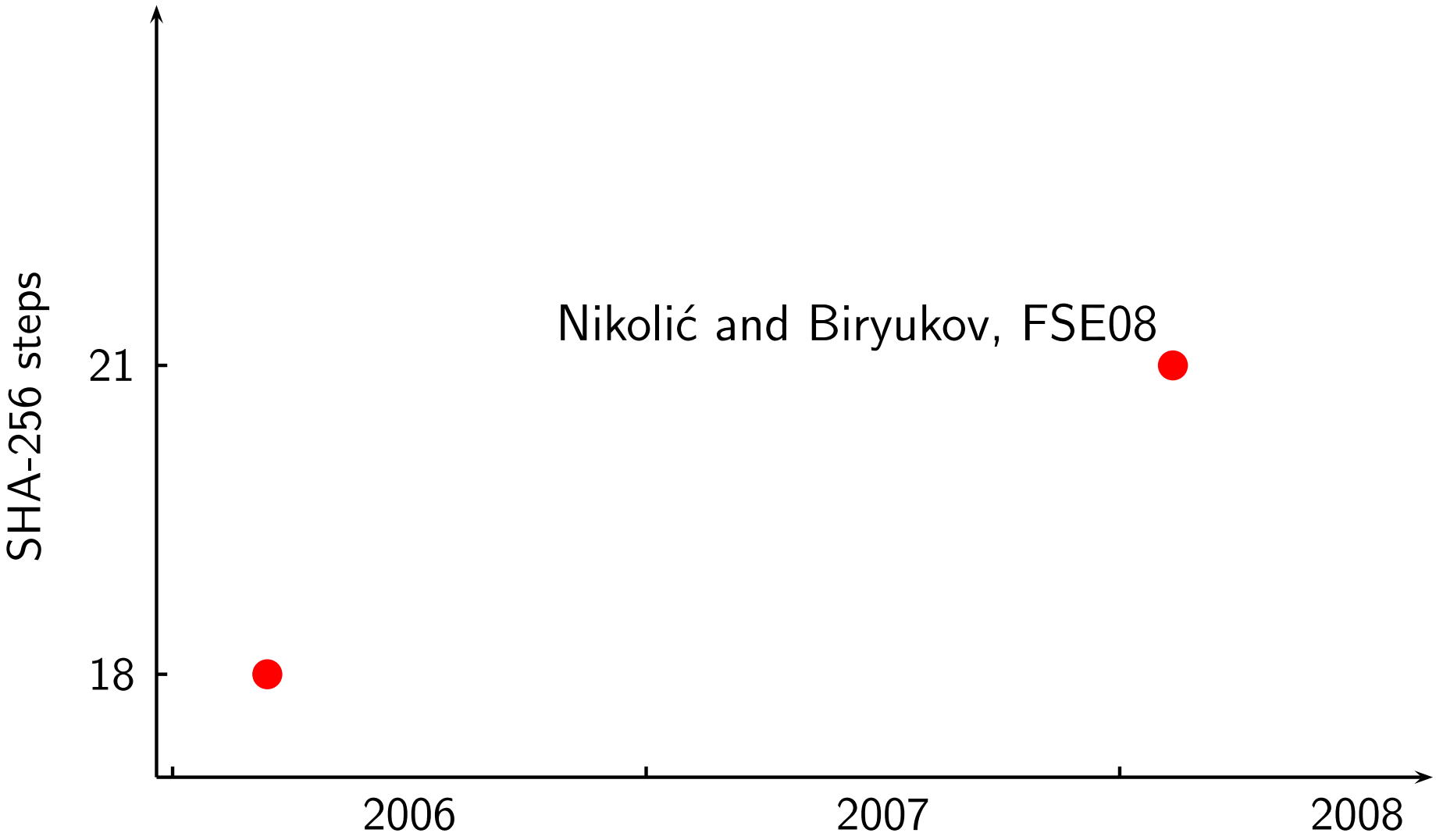
Step-Reduced SHA-256 Collisions



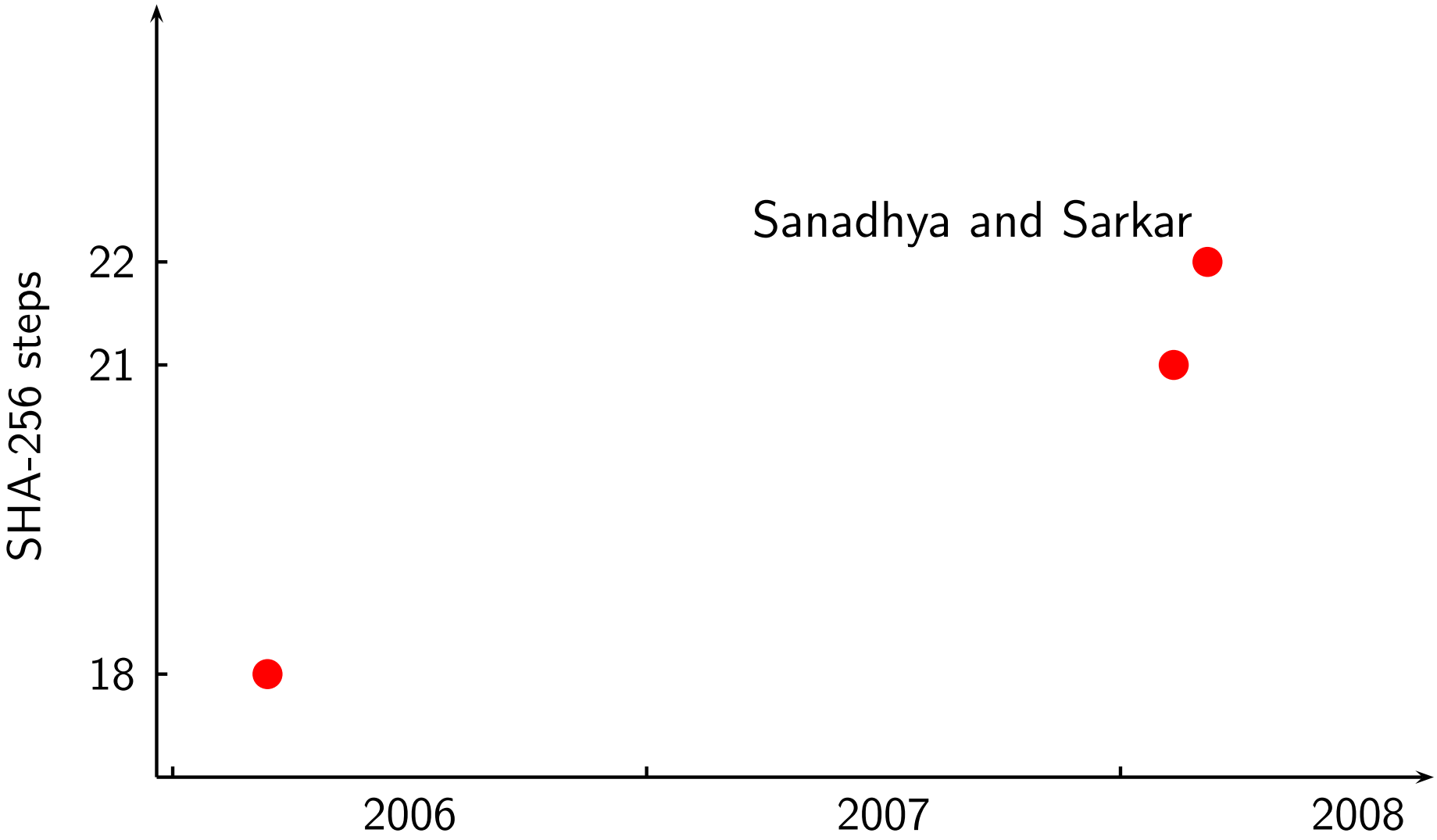
Step-Reduced SHA-256 Collisions



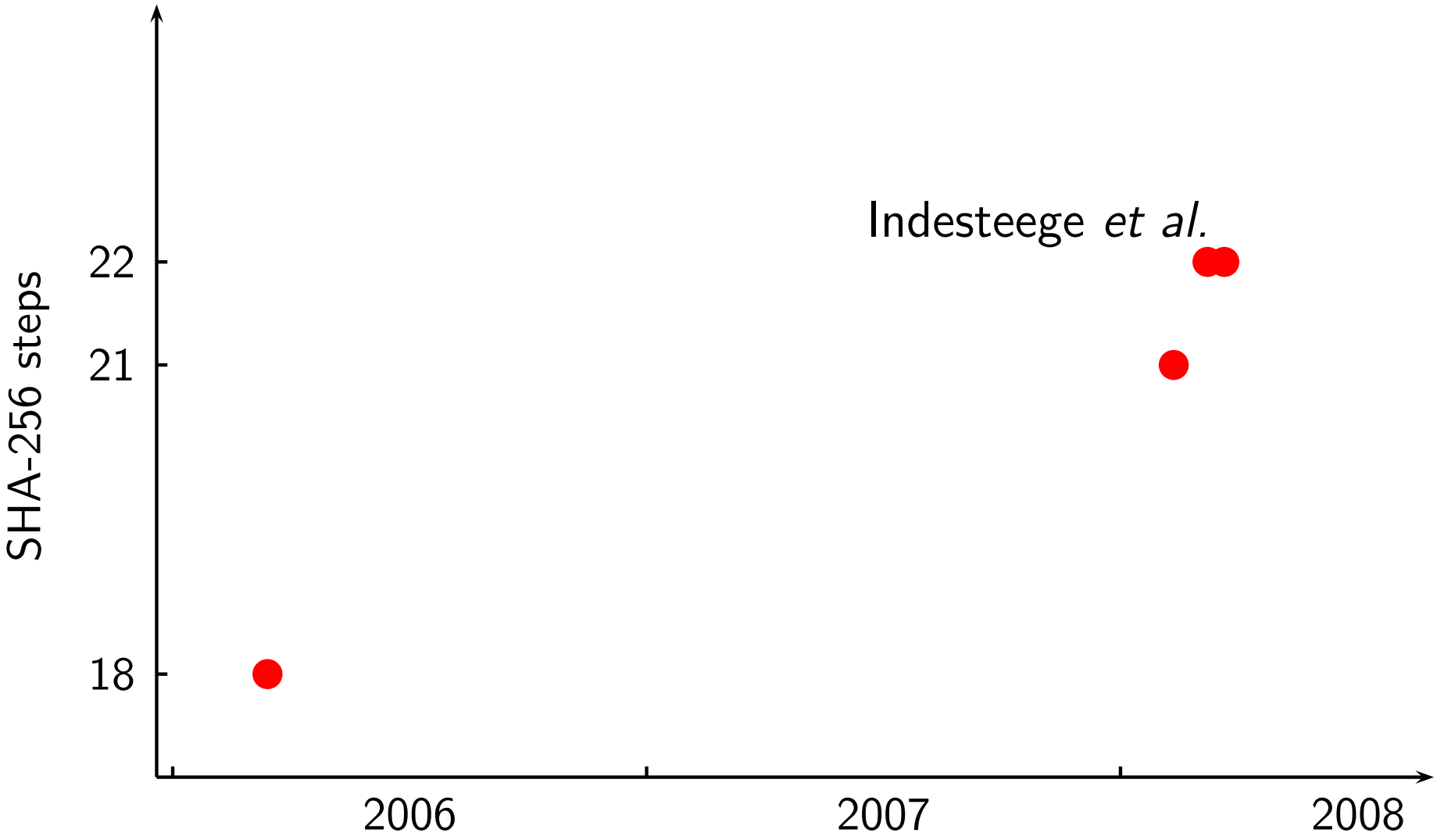
Step-Reduced SHA-256 Collisions



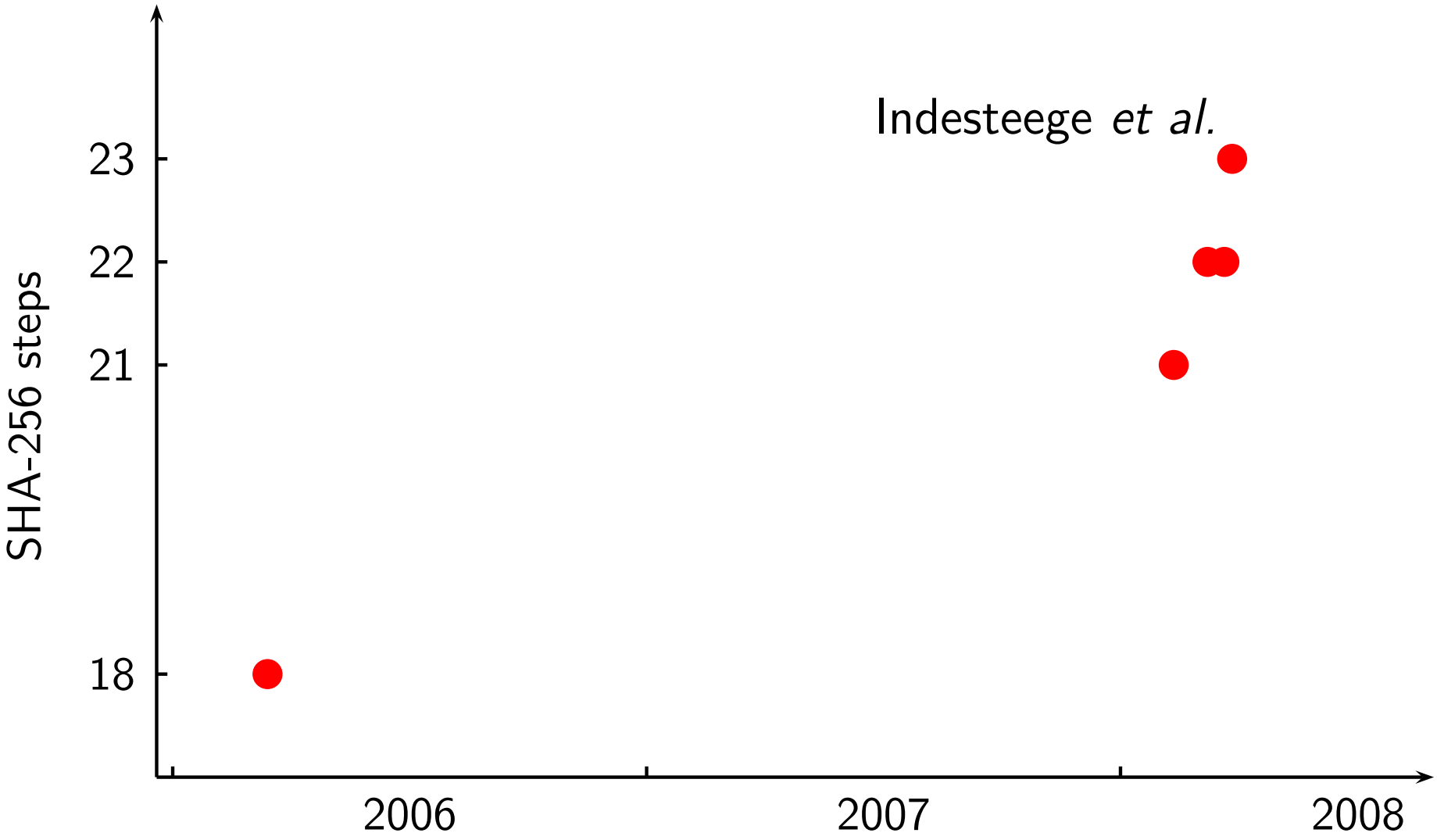
Step-Reduced SHA-256 Collisions



Step-Reduced SHA-256 Collisions



Step-Reduced SHA-256 Collisions



Step-Reduced SHA-256 Collisions

A 24-Step SHA-256 Collision

- **First Message** M

$\texttt{0187e08e}_x$	$\texttt{865cedaf}_x$	$\texttt{5b69e21a}_x$	$\texttt{e0f7485e}_x$
$\texttt{50b98993}_x$	$\texttt{217e4650}_x$	$\texttt{51e3cf65}_x$	$\texttt{c2997c68}_x$
$\texttt{2c267e16}_x$	$\texttt{82ffa4e9}_x$	$\texttt{37b5af09}_x$	$\texttt{5b28721d}_x$
$\texttt{1be35597}_x$	$\texttt{7ff22aa1}_x$	$\texttt{e807a758}_x$	$\texttt{c1519aaa}_x$

- **Second Message** $M^\star$

$\texttt{0187e08e}_x$	$\texttt{865cedaf}_x$	$\texttt{5b69e21a}_x$	$\texttt{e0f7485e}_x$
$\texttt{50b98993}_x$	$\texttt{217e4650}_x$	$\texttt{51e3cf65}_x$	$\texttt{c2997c68}_x$
$\texttt{2c267e16}_x$	$\texttt{82ffa4e9}_x$	$\texttt{37b5af0a}_x$	$\texttt{5b28721c}_x$
$\texttt{1be3f597}_x$	$\texttt{82f24aa0}_x$	$\texttt{e807a758}_x$	$\texttt{c1519aaa}_x$

- $\textbf{SHA256}_{24}(M) = \textbf{SHA256}_{24}(M^\star) =$

$\texttt{1584074c}_x$	$\texttt{8b810a94}_x$	$\texttt{01ea31b1}_x$	$\texttt{81bffd02}_x$
$\texttt{d29c817d}_x$	$\texttt{e4e04b51}_x$	$\texttt{b9f5ac4f}_x$	$\texttt{6b34d1f8}_x$

Conclusions

- **Practical collisions for up to 24-step SHA-256**
- Free-start collisions for 25-step SHA-224
- Free-start near collisions for up to 31-step SHA-256

Sebastiaan Indesteege, Florian Mendel, Bart Preneel and Christian Rechberger
Collisions and other Non-Random Properties for Step-Reduced SHA-256
Cryptology ePrint Archive, Report 2008/131
http://eprint.iacr.org/2008/131