Constant-time $\approx 2^{128}$-security DH on Intel Sandy Bridge

cycles	ladder	open	g	field	source
194036	yes	yes	1	$2^{255} - 19$	CHES 2011
153000?	yes	no	1	$2^{252} - 2^{232} - 1$	eprint 2012
137000?	no	no	1	$(2^{127} - 5997)^2$	Asiacrypt 2012
122716	yes	yes	2	$2^{127} - 1$	Eurocrypt 2013
119904	no	yes	1	2^{254}	CHES 2013
96000?	no	no	1	$(2^{127} - 5997)^2$	CT-RSA 2014
92000?	no	no	1	$(2^{127} - 5997)^2$	eprint 2014
88916	**yes**	**yes**	**2**	$2^{127} - 1$	**Asiacrypt 2014**

CHES 2011: Bernstein–Duif–Lange–Schwabe–Yang. eprint 2012: Hamburg. CHES 2012: Bernstein–Schwabe. Asiacrypt 2012: Longa–Sica. Eurocrypt 2013: Bos–Costello–Hisil–Lauter. CHES 2013: Oliveira–López–Aranha–Rodríguez-Henríquez. CT-RSA 2014, eprint 2014: Faz-Hernández–Longa–Sánchez. Eurocrypt 2014: Costello–Hisil–Smith. **Asiacrypt 2014: Bernstein–Chuengsatiansup–Lange–Schwabe.**

Constant-time $\approx 2^{128}$-security DH on more CPUs

arch	cycles	ladder	open	g	field	source
A8-slow	497389	yes	yes	1	$2^{255}-19$	CHES 2012
A8-slow	305395	yes	yes	2	$2^{127}-1$	**Asiacrypt 2014**
A8-fast	460200	yes	yes	1	$2^{255}-19$	CHES 2012
A8-fast	273349	yes	yes	2	$2^{127}-1$	**Asiacrypt 2014**
Ivy	182708	yes	yes	1	$2^{255}-19$	CHES 2011
Ivy	145000?	yes	yes	1	$(2^{127}-1)^2$	Eurocrypt 2014
Ivy	119032	yes	yes	2	$2^{127}-1$	Eurocrypt 2013
Ivy	114036	no	yes	1	2^{254}	CHES 2013
Ivy	92000?	no	no	1	$(2^{127}-5997)^2$	CT-RSA 2014
Ivy	89000?	no	no	1	$(2^{127}-5997)^2$	eprint 2014
Ivy	88448	yes	yes	2	$2^{127}-1$	**Asiacrypt 2014**
Haswell	145907	yes	yes	1	$2^{255}-19$	CHES 2011
Haswell	100895	yes	yes	2	$2^{127}-1$	Eurocrypt 2013
Haswell	55595	no	yes	1	2^{254}	CHES 2013
Haswell	54389	yes	yes	2	$2^{127}-1$	**Asiacrypt 2014**