WIKIPEDIA
The Free Encyclopedia

Dual_EC_DRBG

Dual_EC_DRBG (**Dual Elliptic Curve Deterministic Random Bit Generator**)[1] is an algorithm that was presented as a cryptographically secure pseudorandom number generator (CSPRNG) using methods in elliptic curve cryptography. Despite wide public criticism, including the public identification of the possibility that the National Security Agency put a backdoor into a recommended implementation, it was, for seven years, one of four CSPRNGs standardized in NIST SP 800-90A as originally published circa June 2006, until it was withdrawn in 2014.

Weakness: a potential backdoor

Weaknesses in the cryptographic security of the algorithm were known and publicly criticised well before the algorithm became part of a formal standard endorsed by the ANSI, ISO, and formerly by the National Institute of Standards and Technology (NIST). One of the weaknesses publicly identified was the potential of the algorithm to harbour a cryptographic backdoor advantageous to those who know about it—the United States government's National Security Agency (NSA)—and no one else. In 2013, *The New York Times* reported that documents in their possession but never released to the public "appear to confirm" that the backdoor was real, and had been deliberately inserted by the NSA as part of its Bullrun decryption program. In December 2013, a Reuters news article alleged that in 2004, before NIST standardized Dual_EC_DRBG, NSA paid RSA Security $10 million in a secret deal to use Dual_EC_DRBG as the default in the RSA BSAFE cryptography library, which resulted in RSA Security becoming the most important distributor of the insecure algorithm.[2] RSA responded that they "categorically deny" that they had ever knowingly colluded with the NSA to adopt an algorithm that was known to be flawed, but also stated "we have never kept [our] relationship [with the NSA] a secret".[3]

Sometime before its first known publication in 2004, a possible kleptographic backdoor was discovered with the Dual_EC_DRBG's design, with the design of Dual_EC_DRBG having the unusual property that it was theoretically impossible for anyone but Dual_EC_DRBG's designers (NSA) to confirm the backdoor's existence. Bruce Schneier concluded shortly after standardization that the "rather obvious" backdoor (along with other deficiencies) would mean that nobody would use Dual_EC_DRBG.[4] The backdoor would allow NSA to decrypt for example SSL/TLS encryption which used Dual_EC_DRBG as a CSPRNG.[5]

Members of the ANSI standard group to which Dual_EC_DRBG was first submitted were aware of the exact mechanism of the potential backdoor and how to disable it,[6] but did not elect to disable or publicize the backdoor. The general cryptographic community was initially not aware of the potential backdoor, until Dan Shumow and Niels Ferguson's publication, or of Certicom's Daniel R. L. Brown and Scott Vanstone's 2005 patent application describing the backdoor mechanism.

In September 2013, *The New York Times* reported that internal NSA memos leaked by Edward Snowden indicated that the NSA had worked during the standardization process to eventually become the sole editor of the Dual_EC_DRBG standard,[7] and concluded that the Dual_EC_DRBG standard did indeed contain a backdoor for the NSA.[8] In response, NIST stated that "NIST would not deliberately weaken a cryptographic standard",[9] but according to the *New York Times* story, the NSA had been spending $250 million per year to insert backdoors in software and hardware as part of the Bullrun program.[10] A Presidential advisory committee subsequently set up to examine NSA's conduct recommended among other things that the US government "fully support and not undermine efforts to create encryption standards".[11]

On April 21, 2014, NIST withdrew Dual_EC_DRBG from its draft guidance on random number generators recommending "current users of Dual_EC_DRBG transition to one of the three remaining approved algorithms as quickly as possible."[12]

Timeline of Dual_EC_DRBG

Time	What happened
May 1997	Adam L. Young and Moti Yung present their cryptovirology paper "Kleptography: Using Cryptography Against Cryptography" at Eurocrypt 1997.[13] The paper shows how to build a covert key exchange into the Diffie–Hellman key exchange protocol. The EC-DRBG backdoor is, with only a trivial modification, equivalent to the Young–Yung backdoor in Diffie–Hellman from Eurocrypt 1997.
August 1997	Adam L. Young and Moti Yung present their cryptovirology paper "The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems" at Crypto 1997.[14] The paper presents a recipe on how to build asymmetric backdoors into crypto algorithms based on discrete logs. The paper generalizes the paradigm used to attack Diffie–Hellman from Eurocrypt 1997. The paper introduces the 'discrete log kleptogram' that would later be designed into the EC-DRBG.
ANSI X9.82 standardization process kicks off in the early 2000s	NSA drives to include Dual_EC_DRBG in ANSI X9.82, when the standardization process kicks off in the early 2000s.[6]
After the ANSI X9.82 standardization process kicked off and before NIST publication	According to John Kelsey (who was listed as author of NIST SP 800-90A together with Elaine Barker), the possibility of the backdoor by carefully chosen *P* and *Q* values was brought up at an ANSI X9.82 meeting. As a result, a way was specified for implementers to choose their own *P* and *Q* values.[15] It turned out later that the specific subtle formulation that NIST put into the standard meant that users could only get the crucial FIPS 140-2 validation of their implementation if they used the original compromised *P* and *Q* values.[16]
October 2003	Goh, Boneh, Pinkas and Golle publish a research paper on the problem of adding key recovery to the SSL/TLS and SSH protocols.[17] They state "The government can convince major software vendors to distribute SSL/TLS or SSH2 implementations with hidden and unfilterable key recovery... Users will not notice the key recovery mechanism because the scheme is hidden." They then suggest that when the server needs a random nonce it can use instead an encryption of the session key computed under the escrow key. This does not leverage an elliptic curve discrete-log kleptogram and as a result requires a large-bandwidth subliminal channel to pull off.
June 2004	A draft (http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=D96134C539F238DD741A65F49189E076?doi=10.1.1.6.1272&rep=rep1&type=pdf) of ANSI X9.82, Part 3 is published, which includes Dual_EC_DRBG.[6] It is unknown if earlier drafts were published.
Sometime in 2004	RSA makes Dual_EC_DRBG the default CSPRNG in BSAFE. In 2013, Reuters reports this is a result of a secret $10 million deal with NSA.[2]
21 January 2005	Priority date of a patent application[18] by the two Certicom members of the ANSI X9.82 standardization committee. The patent describes the working of an elliptic curve CSPRNG backdoor identical to the potential backdoor in Dual_EC_DRBG, and ways to neutralize such a hidden backdoor by choosing alternative curve points and more bit truncation in the output function.[6]
Sometime in 2005[19]	ISO/IEC 18031:2005 is published, and includes Dual_EC_DRBG.[6]
December 2005[20]	The first draft of NIST SP 800-90A is released to the public, includes Dual_EC_DRBG.[5]
16 March 2006	Kristian Gjøsteen publishes *Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005* showing that part of Dual_EC_DRBG is "not cryptographically sound", and constructing a bit-predictor with an advantage of 0.0011, which is considered unacceptable for a CSPRNG.[5][20]

29 March 2006	Daniel R. L. Brown publishes "*Conjectured Security of the ANSI-NIST Elliptic Curve RNG* (http://eprint.iacr.org/2006/117)", concluding that "[Dual_EC_DRBG] should be a serious consideration", assuming less truncation of the curve points than is present in Dual_EC_DRBG, as shown necessary by Gjøsteen's 2006 paper. The paper also anticipates Shumow and Ferguson's 2007 announcement of a possible backdoor: "This proof makes essential use of Q being random. The reason for this is more than just to make the proof work. If Q is not random, then it may be the case the adversary knows a d such that $dQ = P$. Then $dR_i = dS_{i+1}$, so that such a distinguisher could immediately recover the secret prestates from the output. Once the distinguisher gets the prestates, it can easily distinguish the output from random. Therefore, it is generally preferable for Q to be chosen randomly, relative to P."[21]
29 May 2006	Berry Schoenmakers and Andrey Sidorenko publish a *Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator*, showing that empirically the output from Dual_EC_DRBG can be distinguished from random bits, concluding that Dual_EC_DRBG is insecure as a CSPRNG. Note that this is a separate problem from the backdoor. The authors also point out that the security claim of the Dual_EC_DRBG is only supported by informal discussion. No proof of security (e.g., via a reduction argument) is given.[22] It follows that NIST ignored the provably secure pseudorandom number generators that had long existed in the peer-reviewed academic literature.
June 2006	NIST SP 800-90A is published, includes Dual_EC_DRBG with the defects pointed out by Kristian Gjøsteen and Berry Schoenmakers and Andrey Sidorenko not having been fixed.
June 2007	Young and Yung publish a research paper detailing a provably secure asymmetric backdoor in SSL.[23] The asymmetric backdoor utilizes a twisted pair of elliptic curves resulting in a discrete log kleptogram that easily fits into the hello nonce. The attack is an attack on SSL random number generation. The act of generating a hello nonce using the EC-DRBG that NIST backdoored mimics exactly this attack on SSL by Young and Yung.
August 2007	Dan Shumow and Niels Ferguson give an informal presentation demonstrating that an attacker with the backdoor and a small amount of output can completely recover the internal state of EC-DRBG, and therefore predict all future output.[24]
15 November 2007	Bruce Schneier publishes an article with the title "*Did NSA Put a Secret Backdoor in New Encryption Standard?*" in *Wired*, based on Dan Shumow and Niels Ferguson's presentation.[4]
6 June 2013	The first news stories (unrelated to Dual_EC_DRBG) based on Edward Snowden's leak of NSA documents are published.
5 September 2013	Existence of NSA's Bullrun program is revealed, based on the Snowden leaks. One of the purposes of Bullrun is described as being "*to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world.*" *The New York Times* states that "the N.S.A. had inserted a back door into a 2006 standard adopted by N.I.S.T... called the Dual EC DRBG standard",[25] confirming that NSA carried out a malicious software attack.
10 September 2013	Gail Porter, director of the NIST Public Affairs Office, released a statement, saying that "NIST would not deliberately weaken a cryptographic standard."[26] The statement does not address the fact that NIST ultimately ignored the warning about a possible backdoor in the standard from NIST's own cryptographer, John Kelsey.
19 September 2013	RSA Security advises its customers to stop using Dual_EC_DRBG in RSA Security's *BSAFE* toolkit and *Data Protection Manager*, citing NIST guidance made Sept. 12, 2013 that indicated: "NIST strongly recommends that, pending the resolution of the security concerns and the re-issuance of SP 800-90A, the Dual_EC_DRBG, as specified in the January 2012 version of SP 800-90A, no longer be used."[27] Initial media reports cast suspicion over RSA's continued use of Dual_EC_DRBG as the default in its BSAFE and Data Protection Manager products, particularly after 2007 in light of previous published concerns over the potential for a backdoor in the algorithm. RSA Chief of Technology Sam Curry writes a short justification for RSA Security's choice to use Dual_EC_DRBG as default, which is widely criticized by cryptographers. Curry does not discuss the later revealed $10 million deal with NSA to use Dual_EC_DRBG.[28]
18 December 2013	A presidential advisory committee set up to examine the NSA recommended that the US government "fully support and not undermine efforts to create encryption standards"[11]
20 December 2013	Reuters reports on the existence of a $10 million deal between RSA and NSA to set Dual_EC_DRBG as the default CSPRNG in BSAFE.[2]
22 December 2013	RSA Security posts statements categorically denying that it "entered into a 'secret contract' with the NSA to incorporate a known flawed random number generator into its BSAFE encryption libraries" though its statements do not deny the existence of a $10 million deal between RSA and the NSA to set Dual_EC_DRBG as the standard in BSAFE.[3] Some news sites such as BBC

	summarize the press release as a direct denial of existence of the $10 million deal,[29] while other commentary point out that it is not clear what claims exactly the carefully worded RSA Security press release is denying, if any.[30][31]
25 February 2014	In his 2014 RSA Conference keynote speech, RSA Security Executive Chairman (and EMC Executive Vice President) Art Coviello implied that RSA Security had not seen merit in the 2006 and 2007 research papers that pointed out flaws in Dual_EC_DRBG until NIST issued guidance to stop using the CSPRNG. Coviello said RSA Security had seen decreasing revenue from encryption, and no longer wanted to expend resources driving encryption research, but as "contributor to and beneficiary of open standards" would trust NIST and NSA guidance, and blamed NSA for tricking the company.[32]
21 April 2014	Following a public comment period and review, NIST removed Dual_EC_DRBG as a cryptographic algorithm from its draft guidance on random number generators, recommending "that current users of Dual_EC_DRBG transition to one of the three remaining approved algorithms as quickly as possible."[12]
August 2014	Checkoway et al. publish a research paper analyzing the practicality of using the EC-DRBG to build an asymmetric backdoor into SSL and TLS.[33]
January 2015	Michael Wertheimer, director of research at the NSA, wrote "With hindsight, NSA should have ceased supporting the Dual EC DRBG algorithm immediately after security researchers discovered the potential for a trapdoor. In truth, I can think of no better way to describe our failure to drop support for the Dual EC DRBG algorithm as anything other than regrettable."[34]

Description

Overview

The algorithm uses a single integer s as state. Whenever a new random number is requested, this integer is updated. The k-th state is given by

$$s_k = g_P(s_{k-1})$$

The returned random integer r is a function of the state. The k-th random number is

$$r_k = g_Q(s_k)$$

The function $g_P(x)$ depends on the fixed elliptic curve point P. $g_Q(x)$ is similar except that it uses the point Q. The points P and Q stay constant for a particular implementation of the algorithm.

Details

The algorithm allows for different constants, variable output length and other customization. For simplicity, the one described here will use the constants from curve P-256 (one of the 3 sets of constants available) and have fixed output length. The algorithm operates exclusively over a prime finite field $\boldsymbol{F_p}$ ($\mathbb{Z}/p\mathbb{Z}$) where p is prime. The state, the seed and the random numbers are all elements of this field. Field size is

$$p = \texttt{ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551}_{16}$$

An elliptic curve over $\boldsymbol{F_p}$ is given

$$y^2 = x^3 - 3x + b$$

where the constant b is

$$b = \texttt{5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b}_{16}$$

The points on the curve are $E(F_p)$. Two of these points are given as the fixed points P and Q

$$P, Q \in E(F_p)$$

Their coordinates are

$$\begin{aligned}
P_x &= \texttt{6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296}_{16} \\
P_y &= \texttt{4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5}_{16} \\
Q_x &= \texttt{c97445f4 5cdef9f0 d3e05e1e 585fc297 235b82b5 be8ff3ef ca67c598 52018192}_{16} \\
Q_y &= \texttt{b28ef557 ba31dfcb dd21ac46 e2a91e3c 304f44cb 87058ada 2cb81515 1e610046}_{16}
\end{aligned}$$

A function to extract the x-coordinate is used. It "converts" from elliptic curve points to elements of the field.

$$X(x, y) = x$$

Output integers are truncated before being output

$$t(x) = x \bmod \frac{p}{2^{16}}$$

The functions g_P and g_Q. These functions raise the fixed points to a power. "Raising to a power" in this context, means using the special operation defined for points on elliptic curves.

$$g_P(x) = X(P^x)$$

$$g_Q(x) = t(X(Q^x))$$

The generator is seeded with an element from F_p

$$s_1 = g_P(seed)$$

The k-th state and random number

$$s_k = g_P(s_{k-1})$$

$$r_k = g_Q(s_k)$$

The random numbers

$$r_1, r_2, \ldots$$

Security

The stated purpose of including the Dual_EC_DRBG in NIST SP 800-90A is that its security is based on computational hardness assumptions from number theory. A mathematical security reduction proof can then prove that as long as the number theoretical problems are hard, the random number generator itself is secure. However, the makers of Dual_EC_DRBG did not publish a security reduction for Dual_EC_DRBG, and it was shown soon after the NIST draft was published that Dual_EC_DRBG was indeed not secure, because it output too many bits per round.[22][35][36] The output of too many bits (along with carefully chosen elliptic curve points P and Q) is what makes the NSA backdoor possible, because it enables the attacker to revert the truncation by brute force guessing. The output of too many bits was not corrected in the final published standard, leaving Dual_EC_DRBG both insecure and backdoored.[5]

In many other standards, constants that are meant to be arbitrary are chosen by the *nothing up my sleeve number* principle, where they are derived from pi or similar mathematical constants in a way that leaves little room for adjustment. However, Dual_EC_DRBG did not specify how the default *P* and *Q* constants were chosen, possibly because they were constructed by NSA to be backdoored. Because the standard committee were aware of the potential for a backdoor, a way for an implementer to choose their own secure *P* and *Q* was included.[6][15] But the exact formulation in the standard was written such that use of the alleged backdoored *P* and *Q* was required for FIPS 140-2 validation, so the OpenSSL project chose to implement the backdoored *P* and *Q*, even though they were aware of the potential backdoor and would have preferred generating their own secure *P* and *Q*.[37] New York Times would later write that NSA had worked during the standardization process to eventually become the sole editor of the standard.[7]

A security proof was later published for Dual_EC_DRBG by Daniel R.L. Brown and Kristian Gjøsteen, showing that the generated elliptic curve points would be indistinguishable from uniformly random elliptic curve points, and that if fewer bits were output in the final output truncation, and if the two elliptic curve points *P* and *Q* were independent, then Dual_EC_DRBG is secure. The proof relied on the assumption that three problems were hard: the *decisional Diffie–Hellman assumption* (which is generally accepted to be hard), and two newer less-known problems which are not generally accepted to be hard: the *truncated point problem*, and the *x-logarithm problem*.[35][36] Dual_EC_DRBG was quite slow compared to many alternative CSPRNGs (which don't have security reductions[38]), but Daniel R.L. Brown argues that the security reduction makes the slow Dual_EC_DRBG a valid alternative (assuming implementors disable the obvious backdoor).[38] Note that Daniel R.L. Brown works for Certicom, the main owner of elliptic curve cryptography patents, so there may be a conflict of interest in promoting an EC CSPRNG.

The alleged NSA backdoor would allow the attacker to determine the internal state of the random number generator from looking at the output from a single round (32 bytes); all future output of the random number generator can then easily be calculated, until the CSPRNG is reseeded with an external source of randomness. This makes for example SSL/TLS vulnerable, since the setup of a TLS connection includes the sending of a randomly generated cryptographic nonce in the clear.[5] NSA's alleged backdoor would depend on their knowing of the single *e* such that $eQ = P$. This is a hard problem if *P* and *Q* are set ahead of time, but it's easier if *P* and *Q* are chosen.[24] *e* is a secret key presumably known only by NSA, and the alleged backdoor is a kleptographic asymmetric hidden backdoor.[39] Matthew Green's blog post *The Many Flaws of Dual_EC_DRBG*[40] has a simplified explanation of how the alleged NSA backdoor works by employing the discrete-log kleptogram introduced in Crypto 1997.[14]

Standardization and implementations

NSA first introduced Dual_EC_DRBG in the ANSI X9.82 DRBG in the early 2000s, including the same parameters which created the alleged backdoor, and Dual_EC_DRBG was published in a draft ANSI standard. Dual_EC_DRBG also exists in the ISO 18031 standard.[6]

According to John Kelsey (who together with Elaine Barker was listed as author of NIST SP 800-90A), the possibility of the backdoor by carefully chosen *P* and *Q* was brought up at an ANSI X9F1 Tool Standards and Guidelines Group meeting.[6] When Kelsey asked Don Johnson of Cygnacom about the origin of *Q*, Johnson answered in a 27 October 2004 email to Kelsey that NSA had prohibited the public discussion of generation of an alternative *Q* to the NSA-supplied one.[41]

At least two members of the Members of the ANSI X9F1 Tool Standards and Guidelines Group which wrote ANSI X9.82, Daniel R. L. Brown and Scott Vanstone from Certicom,[6] were aware of the exact circumstances and mechanism in which a backdoor could occur, since they filed a patent application[18] in January 2005 on exactly how to insert or prevent the backdoor in DUAL_EC_DRBG. The working of the "trap door" mentioned in the patent is identical to the one later confirmed in Dual_EC_DRBG. Writing about the patent in 2014, commentator Matthew Green describes the patent as a "passive aggressive" way of spiting NSA by publicizing the backdoor, while still criticizing everybody on the committee for not actually disabling the backdoor they obviously were aware of.[41] Brown and Vanstone's patent list two necessary conditions for the backdoor to exist:

1) Chosen *Q*

> An elliptic curve random number generator avoids escrow keys by choosing a point *Q* on the elliptic curve as verifiably random. Intentional use of escrow keys can provide for back up functionality. The relationship between *P* and *Q* is used as an escrow key and stored by for a security domain. The administrator logs the output of the generator to reconstruct the random number with the escrow key.

2) Small output truncation

> [0041] Another alternative method for preventing a key escrow attack on the output of an ECRNG, shown in Figures 3 and 4 is to add a truncation function to ECRNG to truncate the ECRNG output to approximately half the length of a compressed elliptic curve point. Preferably, this operation is done in addition to the preferred method of Figure 1 and 2, however, it will be appreciated that it may be performed as a primary measure for preventing a key escrow attack. The benefit of truncation is that the list of R values associated with a single ECRNG output r is typically infeasible to search. For example, for a 160-bit elliptic curve group, the number of potential points R in the list is about 2^{80}, and searching the list would be about as hard as solving the discrete logarithm problem. The cost of this method is that the ECRNG is made half as efficient, because the output length is effectively halved.

According to John Kelsey, the option in the standard to choose a verifiably random *Q* was added as an option in response to the suspected backdoor,[15] though in such a way that FIPS 140-2 validation could only be attained by using the possibly backdoored *Q*.[37] Steve Marquess (who helped implement NIST SP 800-90A for OpenSSL) speculated that this requirement to use the potentially backdoored points could be evidence of NIST complicity.[42] It is not clear why the standard did not specify the default *Q* in the standard as a verifiably generated nothing up my sleeve number, or why the standard did not use greater truncation, which Brown's patent said could be used as the "primary measure for preventing a key escrow attack". The small truncation was unusual compared to previous EC PRGs, which according to Matthew Green had only output 1/2 to 2/3 of the bits in the output function.[5] The low truncation was in 2006 shown by Gjøsteen to make the RNG predictable and therefore unusable as a CSPRNG, even if *Q* had not been chosen to contain a backdoor.[20] The standard says that implementations "should" use the small max_outlen provided, but gives the option of outputting a multiple of 8 fewer bits. Appendix C of the standard gives a loose argument that outputting fewer bits will make the output less uniformly distributed. Brown's 2006 security proof relies on outlen being much smaller the default max_outlen value in the standard.

The ANSI X9F1 Tool Standards and Guidelines Group which discussed the backdoor also included three employees from the prominent security company RSA Security.[6] In 2004, RSA Security made an implementation of Dual_EC_DRBG which contained the NSA backdoor the default CSPRNG in their RSA BSAFE as a result of a secret $10 million deal with NSA. In 2013, after the New York Times reported that Dual_EC_DRBG contained a backdoor by the NSA, RSA Security said they had not been aware of any backdoor when they made the deal with NSA, and told their customers to switch CSPRNG. In the 2014 RSA Conference keynote, RSA Security Executive Chairman Art Coviello explained that RSA had seen declining revenue from encryption, and had decided to stop being "drivers" of independent encryption research, but to instead to "put their trust behind" the standards and guidance from standards organizations such as NIST.[32]

A draft of NIST SP 800-90A including the Dual_EC_DRBG was published in December 2005. The final NIST SP 800-90A including Dual_EC_DRBG was published in June 2006. Documents leaked by Snowden have been interpreted as suggesting that the NSA backdoored Dual_EC_DRBG, with those making the allegation citing the NSA's work during the standardization process to eventually become the sole editor of the standard.[7] The early usage of Dual_EC_DRBG by RSA Security (for which NSA was later reported to have secretly paid $10 million) was cited by the NSA as an argument for Dual_EC_DRBG's acceptance into the NIST SP 800-90A standard.[2] RSA Security subsequently cited Dual_EC_DRBG's acceptance into the NIST standard as a reason they used Dual_EC_DRBG.[43]

Daniel R. L. Brown's March 2006 paper on the security reduction of Dual_EC_DRBG mentions the need for more output truncation and a randomly chosen *Q*, but mostly in passing, and does not mention his conclusions from his patent that these two defects in Dual_EC_DRBG together can be used as a backdoor. Brown writes in the conclusion: "Therefore, the ECRNG should be a serious consideration, and its high efficiency makes it suitable even for constrained environments." Note that others have criticised Dual_EC_DRBG as being extremely slow, with Bruce Schneier concluding "It's too slow for anyone to willingly use it",[4] and Matthew Green saying Dual_EC_DRBG is "Up to a thousand times slower" than the alternatives.[5] The potential for a backdoor in Dual_EC_DRBG was not widely publicised outside of internal standard group meetings. It was only after Dan Shumow and Niels Ferguson's 2007 presentation that the potential for a backdoor became widely known. Shumow and Ferguson had been tasked with implementing Dual_EC_DRBG for Microsoft, and at least Furguson had discussed the possible backdoor in a 2005 X9 meeting.[15] Bruce Schneier wrote in a 2007 Wired article that the Dual_EC_DRBG's flaws were so obvious that nobody would use Dual_EC_DRBG: "It makes no sense as a trap door: It's public, and rather obvious. It makes no sense from an engineering perspective: It's too slow for anyone to willingly use it."[4] Schneier was apparently unaware that RSA Security had used Dual_EC_DRBG as the default in BSAFE since 2004.

OpenSSL implemented all of NIST SP 800-90A including Dual_EC_DRBG at the request of a client. The OpenSSL developers were aware of the potential backdoor because of Shumow and Ferguson's presentation, and wanted to use the method included in the standard to choose a guaranteed non-backdoored *P* and *Q*, but were told that to get FIPS 140-2 validation they would have to use the default *P* and *Q*. OpenSSL chose to implement Dual_EC_DRBG despite its dubious reputation for completeness, noting that OpenSSL tried to be complete and implements many other insecure algorithms. OpenSSL did not use Dual_EC_DRBG as the default CSPRNG, and it was discovered in 2013 that a bug made the OpenSSL implementation of Dual_EC_DRBG non-functioning, meaning that no one could have been using it.[37]

Bruce Schneier reported in December 2007 that Microsoft added Dual_EC_DRBG support to Windows Vista, though not enabled by default, and Schneier warned against the known potential backdoor.[44] Windows 10 and later will silently replace calls to Dual_EC_DRBG with calls to CTR_DRBG based on AES.[45]

On September 9, 2013, following the Snowden leak, and the *New York Times* report on the backdoor in Dual_EC_DRBG, the National Institute of Standards and Technology (NIST) ITL announced that in light of community security concerns, it was reissuing SP 800-90A as draft standard, and re-opening SP800-90B/C for public comment. NIST now "strongly recommends" against the use of Dual_EC_DRBG, as specified in the January 2012 version of SP 800-90A.[46][47] The discovery of a backdoor in a NIST standard has been a major embarrassment for the NIST.[48]

RSA Security had kept Dual_EC_DRBG as the default CSPRNG in BSAFE even after the wider cryptographic community became aware of the potential backdoor in 2007, but there does not seem to have been a general awareness of BSAFE's usage of Dual_EC_DRBG as a user option in the community. Only after widespread concern about the backdoor was there an effort to find software which used Dual_EC_DRBG, of which BSAFE was by far the most prominent found. After the 2013 revelations, RSA security Chief of Technology Sam Curry provided Ars Technica with a rationale for originally choosing the flawed Dual EC DRBG standard as default over the alternative random number generators.[49] The technical accuracy of the statement was widely criticized by cryptographers, including Matthew Green and Matt Blaze.[28] On December 20, 2013, it was reported by Reuters that RSA had accepted a secret payment of $10 million from the NSA to set the Dual_EC_DRBG random number generator as the default in two of its encryption products.[2][50] On December 22, 2013, RSA posted a statement to its corporate blog "categorically" denying a secret deal with the NSA to insert a "known flawed random number generator" into its BSAFE toolkit [3]

Following the New York Times story asserting that Dual_EC_DRBG contained a backdoor, Brown (who had applied for the backdoor patent and published the security reduction) wrote an email to an IETF mailing list defending the Dual_EC_DRBG standard process:[38]

> 1. Dual_EC_DRBG, as specified in NIST SP 800-90A and ANSI X9.82-3, allows an alternative choice of constants *P* and *Q*. As far as I know, the alternatives do not admit a known feasible backdoor. In my view, it is incorrect to imply that Dual_EC_DRBG always has a backdoor, though I admit a wording to qualify the affected cases may be awkward.
>
> 2. Many things are obvious in hindsight. I'm not sure if this was obvious. [...]
>
> 8. All considered, I don't see how the ANSI and NIST standards for Dual_EC_DRBG can be viewed as a subverted standard, per se. But maybe that's just because I'm biased or naive.
>
> —Daniel Brown, [38]

Software and hardware which contained the possible backdoor

Implementations which used Dual_EC_DRBG would usually have gotten it via a library. At least RSA Security (BSAFE library), OpenSSL, Microsoft, and Cisco[51] have libraries which included Dual_EC_DRBG, but only BSAFE used it by default. According to the Reuters article which revealed the secret $10 million deal between RSA Security and NSA, RSA Security's BSAFE was the most important distributor of the algorithm.[2] There was a flaw in OpenSSL's implementation of Dual_EC_DRBG that made it non-working outside test mode, from which OpenSSL's Steve Marquess concludes that nobody used OpenSSL's Dual_EC_DRBG implementation.[37]

A list of products which have had their CSPRNG-implementation FIPS 140-2 validated is available at the NIST.[52] The validated CSPRNGs are listed in the Description/Notes field. Note that even if Dual_EC_DRBG is listed as validated, it may not have been enabled by default. Many implementations come from a renamed copy of a library implementation.[53]

The BlackBerry software is an example of non-default use. It includes support for Dual_EC_DRBG, but not as default. BlackBerry Ltd has however not issued an advisory to any of its customers who may have used it, because they do not consider the probable backdoor a vulnerability.[54] Jeffrey Carr quotes a letter from Blackberry:[54]

> The Dual EC DRBG algorithm is only available to third party developers via the Cryptographic APIs on the [Blackberry] platform. In the case of the Cryptographic API, it is available if a 3rd party developer wished to use the functionality and explicitly designed and developed a system that requested the use of the API.

Bruce Schneier has pointed out that even if not enabled by default, having a backdoored CSPRNG implemented as an option can make it easier for NSA to spy on targets which have a software-controlled command-line switch to select the encryption algorithm, or a "registry" system, like most Microsoft products, such as Windows Vista:

> A Trojan is really, really big. You can't say that was a mistake. It's a massive piece of code collecting keystrokes. But changing a bit-one to a bit-two [in the registry to change the default random number generator on the machine] is probably going to be undetected. It is a low conspiracy, highly deniable way of getting a backdoor. So there's a benefit to getting it into the library and into the product.
>
> —Bruce Schneier, [51]

In December 2013, a proof of concept backdoor[39] was published that uses the leaked internal state to predict subsequent random numbers, an attack viable until the next reseed.

In December 2015, Juniper Networks announced[55] that some revisions of their ScreenOS firmware used Dual_EC_DRBG with the suspect *P* and *Q* points, creating a backdoor in their firewall. Originally it was supposed to use a Q point chosen by Juniper which may or may not have been generated in provably safe way. Dual_EC_DRBG was then used to seed ANSI X9.17 PRNG. This would have obfuscated the Dual_EC_DRBG output thus killing the backdoor. However, a "bug" in the code exposed the raw output of the Dual_EC_DRBG, hence compromising the security of the system. This backdoor was then backdoored itself by an unknown party which changed the Q point and some test vectors.[56][57][58] Allegations that the NSA had persistent backdoor access through Juniper firewalls had already been published in 2013 by *Der Spiegel*.[59] The kleptographic backdoor is an example of NSA's NOBUS policy, of having security holes that only they can exploit.

See also

- Random number generator attack
- Crypto AG – a Swiss company specialising in communications and information security, who are widely believed to have allowed western security agencies (including NSA) to insert backdoors in their cryptography machines[60]

References

1. Barker, E. B.; Kelsey, J. M. (January 2012). "Recommendations for Random Number Generation Using Deterministic Random Bit Generators (Revised)" (http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf) (PDF). National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-90A (https://doi.org/10.6028%2FNIST.SP.800-90A). NIST SP 800-90. Archived (https://web.archive.org/web/20131009210654/http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf) (PDF) from the original on 2013-10-09. Retrieved 2013-09-11. {{cite journal}}: Cite journal requires |journal= (help)
2. Menn, Joseph (December 20, 2013). "Exclusive: Secret contract tied NSA and security industry pioneer" (https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220). *Reuters*. San Francisco. Archived (https://web.archive.org/web/20150924191918/http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220) from the original on September 24, 2015. Retrieved December 20, 2013.
3. The Security Division of EMC, RSA. "RSA Response to Media Claims Regarding NSA Relationship" (https://web.archive.org/web/20131223121638/http://blogs.rsa.com/news-media-2/rsa-response/). RSA. Archived from the original (https://blogs.rsa.com/news-media-2/rsa-response/) on 23 December 2013. Retrieved 22 December 2013.
4. Bruce Schneier (2007-11-15). "Did NSA Put a Secret Backdoor in New Encryption Standard?" (http://archive.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115). *Wired News*. Archived (https://web.archive.org/web/20140621062515/http://archive.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115) from the original on 2014-06-21.

5. Green, Matthew (2013-09-18). "The Many Flaws of Dual_EC_DRBG" (http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html). Archived (https://web.archive.org/web/20160820174502/http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html) from the original on 2016-08-20. Retrieved 2013-09-22.
6. Green, Matthew (2013-12-28). "A Few Thoughts on Cryptographic Engineering: A few more notes on NSA random number generators" (http://blog.cryptographyengineering.com/2013/12/a-few-more-notes-on-nsa-random-number.html). Blog.cryptographyengineering.com. Archived (https://web.archive.org/web/20160126035830/http://blog.cryptographyengineering.com/2013/12/a-few-more-notes-on-nsa-random-number.html) from the original on 2016-01-26. Retrieved 2015-12-23.
7. Ball, James; Borger, Julian; Greenwald, Glenn (2013-09-06). "Revealed: how US and UK spy agencies defeat internet privacy and security" (https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security). *The Guardian*. Archived (https://web.archive.org/web/20130918135152/http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security) from the original on 2013-09-18. Retrieved 2016-12-14.
8. Perlroth, Nicole (September 10, 2013). "Government Announces Steps to Restore Confidence on Encryption Standards" (http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/). *The New York Times*. Archived (https://web.archive.org/web/20140712084931/http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/) from the original on July 12, 2014. Retrieved September 11, 2013.
9. Swenson, Gayle (2013-09-10). "Cryptographic Standards Statement" (http://www.nist.gov/director/cybersecuritystatement-091013.cfm). *NIST*. Archived (https://web.archive.org/web/20160825235434/http://www.nist.gov/director/cybersecuritystatement-091013.cfm) from the original on 2016-08-25. Retrieved 2018-02-15.
10. "Secret Documents Reveal N.S.A. Campaign Against Encryption" (https://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html). *The New York Times*. 5 September 2013. Archived (https://web.archive.org/web/20180211071327/http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html) from the original on 11 February 2018. Retrieved 1 March 2017.
11. "NSA should stop undermining encryption standards, Obama panel says" (https://arstechnica.com/information-technology/2013/12/nsa-should-stop-undermining-encryption-standards-obama-panel-says/). *Ars Technica*. 2013-12-18. Archived (https://web.archive.org/web/20180304054830/https://arstechnica.com/information-technology/2013/12/nsa-should-stop-undermining-encryption-standards-obama-panel-says/) from the original on 2018-03-04. Retrieved 2017-06-14.
12. "NIST Removes Cryptography Algorithm from Random Number Generator Recommendations" (https://www.nist.gov/itl/csd/sp800-90-042114.cfm). *National Institute of Standards and Technology*. 21 April 2014. Archived (https://web.archive.org/web/20160829031025/http://www.nist.gov/itl/csd/sp800-90-042114.cfm) from the original on 29 August 2016. Retrieved 13 July 2017.
13. Young, Adam; Yung, Moti (1997-05-11). "Kleptography: Using Cryptography Against Cryptography". *Advances in Cryptology — EUROCRYPT '97* (https://www.researchgate.net/publication/221348188). Lecture Notes in Computer Science. Vol. 1233. Springer, Berlin, Heidelberg. pp. 62–74. doi:10.1007/3-540-69053-0_6 (https://doi.org/10.1007%2F3-540-69053-0_6). ISBN 978-3-540-69053-5 – via ResearchGate.
14. Young, Adam; Yung, Moti (1997-08-17). "The prevalence of kleptographic attacks on discrete-log based cryptosystems". *Advances in Cryptology — CRYPTO '97* (https://www.researchgate.net/publication/221354983). Lecture Notes in Computer Science. Vol. 1294. Springer, Berlin, Heidelberg. pp. 264–276. doi:10.1007/bfb0052241 (https://doi.org/10.1007%2Fbfb0052241). ISBN 978-3-540-63384-6 – via ResearchGate.
15. http://csrc.nist.gov/groups/ST/crypto-review/documents/dualec_in_X982_and_sp800-90.pdf Archived (https://web.archive.org/web/20151129045934/http://csrc.nist.gov/groups/ST/crypto-review/documents/dualec_in_X982_and_sp800-90.pdf) 2015-11-29 at the Wayback Machine
16. " 'Flaw in Dual EC DRBG (no, not that one)' – MARC" (https://marc.info/?l=openssl-announce&m=138747119822324&w=2). Marc.info. 2013-12-19. Archived (https://web.archive.org/web/20141016045241/http://marc.info/?l=openssl-announce&m=138747119822324&w=2) from the original on 2014-10-16. Retrieved 2015-12-23.
17. Goh, E. J.; Boneh, D.; Pinkas, B.; Golle, P. (2003). *The design and implementation of protocol-based hidden key recovery*. ISC.

18. US 2007189527 (https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US2007189527), Brown, Daniel R. L. & Vanstone, Scott A., "Elliptic curve random number generation", assigned to Certicom Corp.
19. "ISO/IEC 18031:2005 – Information technology – Security techniques – Random bit generation" (http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=30816). Iso.org. Archived (https://web.archive.org/web/20160303232451/http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=30816) from the original on 2016-03-03. Retrieved 2015-12-23.
20. "Archived copy" (https://web.archive.org/web/20110525081912/http://www.math.ntnu.no/~kristiag/drafts/dual-ec-drbg-comments.pdf) (PDF). Archived from the original (http://www.math.ntnu.no/~kristiag/drafts/dual-ec-drbg-comments.pdf) (PDF) on 2011-05-25. Retrieved 2007-11-16.
21. Daniel R. L. Brown (2006). "Conjectured Security of the ANSI-NIST Elliptic Curve RNG" (http://eprint.iacr.org/2006/117). *Cryptology ePrint Archive*. Archived (https://web.archive.org/web/20071121233227/http://eprint.iacr.org/2006/117) from the original on 2007-11-21. Retrieved 2007-11-16.
22. Schoenmakers, Berry; Sidorenko, Andrey (29 May 2006). "Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator" (http://eprint.iacr.org/2006/190). *Cryptology ePrint Archive*. Archived (https://web.archive.org/web/20071118202807/http://eprint.iacr.org/2006/190) from the original on 18 November 2007. Retrieved 15 November 2007.
23. Adam L. Young, Moti Yung (2007). *Space-Efficient Kleptography Without Random Oracles*. Information Hiding.
24. Shumow, Dan; Ferguson, Niels. "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec PRNG" (http://rump2007.cr.yp.to/15-shumow.pdf) (PDF). Microsoft. Archived (https://web.archive.org/web/20071023134203/http://rump2007.cr.yp.to/15-shumow.pdf) (PDF) from the original on 2007-10-23. Retrieved 2007-11-15.
25. Perlroth, Nicole (10 September 2013). "Government Announces Steps to Restore Confidence on Encryption Standards" (http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/). *The New York Times*. Archived (https://web.archive.org/web/20140712084931/http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/) from the original on 12 July 2014. Retrieved 11 September 2013.
26. "Cryptographic Standards Statement" (https://www.nist.gov/director/cybersecuritystatement-091013.cfm). *NIST*. Nist.gov. 2013-09-10. Archived (https://web.archive.org/web/20130912234248/http://www.nist.gov/director/cybersecuritystatement-091013.cfm) from the original on 2013-09-12. Retrieved 2015-12-23.
27. NIST, National Institute of Standards & Technology. "SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013" (http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf) (PDF). NIST.gov. Archived (https://web.archive.org/web/20130927123145/http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf) (PDF) from the original on 27 September 2013. Retrieved 12 September 2013.
28. Matthew Green (2013-09-20). "RSA warns developers not to use RSA products" (http://blog.cryptographyengineering.com/2013/09/rsa-warns-developers-against-its-own.html?imm_mid=0b0b73&cmp=em-prog-na-na-newsltr_20130928_direct). A Few Thoughts on Cryptographic Engineering. Archived (https://web.archive.org/web/20131229005026/http://blog.cryptographyengineering.com/2013/09/rsa-warns-developers-against-its-own.html?imm_mid=0b0b73&cmp=em-prog-na-na-newsltr_20130928_direct) from the original on 2013-12-29. Retrieved 2013-09-28.
29. "RSA denies link with US spying agency" (https://www.bbc.co.uk/news/technology-25492461). *BBC News*. 23 December 2013. Archived (https://web.archive.org/web/20181106015402/https://www.bbc.co.uk/news/technology-25492461) from the original on 6 November 2018. Retrieved 20 June 2018.
30. "RSA's 'Denial' Concerning $10 Million From The NSA To Promote Broken Crypto Not Really A Denial At All" (https://www.techdirt.com/articles/20131222/23532125671/rsas-denial-concerning-10-million-nsa-to-promote-broken-crypto-not-really-denial-all.shtml). Techdirt. 2013-12-23. Archived (https://web.archive.org/web/20151224104949/https://www.techdirt.com/articles/20131222/23532125671/rsas-denial-concerning-10-million-nsa-to-promote-broken-crypto-not-really-denial-all.shtml) from the original on 2015-12-24. Retrieved 2015-12-23.

31. Goodin, Dan (2013-12-23). "RSA issues non-denying denial of NSA deal to favor flawed crypto code" (https://arstechnica.com/security/2013/12/rsa-issues-non-denying-denial-of-nsa-deal-to-favor-flawed-crypto-code/). *Ars Technica*. Archived (https://web.archive.org/web/20151224103822/http://arstechnica.com/security/2013/12/rsa-issues-non-denying-denial-of-nsa-deal-to-favor-flawed-crypto-code/) from the original on 2015-12-24. Retrieved 2015-12-23.
32. Jeffrey Carr (2014-02-26). "Six Cryptographers Whose Work on Dual EC DRBG Were Deemed Without Merit by RSA Chief Art Coviello" (http://jeffreycarr.blogspot.dk/2014/02/six-cryptographers-whose-work-on-dual.html). Digital Dao. Archived (https://web.archive.org/web/20140303212637/http://jeffreycarr.blogspot.dk/2014/02/six-cryptographers-whose-work-on-dual.html) from the original on 2014-03-03. Retrieved 2014-02-27.
33. S. Checkoway; M. Fredrikson; R. Niederhagen; A. Everspaugh; M. Green; T. Lange; T. Ristenpart; D. J. Bernstein; J. Maskiewicz; H. Shacham (2014). *On the Practical Exploitability of Dual EC in TLS Implementations*. USENIX Security Symposium.
34. https://www.ams.org/journals/notices/201502/rnoti-p165.pdf Archived (https://web.archive.org/web/20220209124927/https://www.ams.org/journals/notices/201502/rnoti-p165.pdf) 2022-02-09 at the Wayback Machine
35. Kristian Gjøsteen. *Comments on Dual-EC-DRBG/NIST SP 800-90* (http://www.math.ntnu.no/~kristiag/drafts/dual-ec-drbg-comments.pdf) Archived (https://web.archive.org/web/20110525081912/http://www.math.ntnu.no/~kristiag/drafts/dual-ec-drbg-comments.pdf) 2011-05-25 at the Wayback Machine
36. Brown, Daniel R. L.; Gjøsteen, Kristian (2007-08-19). "A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator". *Advances in Cryptology - CRYPTO 2007* (https://eprint.iacr.org/2007/048). Lecture Notes in Computer Science. Vol. 4622. Springer, Berlin, Heidelberg. pp. 466–481. doi:10.1007/978-3-540-74143-5_26 (https://doi.org/10.1007%2F978-3-540-74143-5_26). ISBN 978-3-540-74142-8. Archived (https://web.archive.org/web/20180216025221/https://eprint.iacr.org/2007/048) from the original on 2018-02-16. Retrieved 2018-02-15 – via Cryptology ePrint Archive.
37. Steve Marquess. "Flaw in Dual EC DRBG (no, not that one)" (https://marc.info/?l=openssl-announce&m=138747119822324). OpenSSL project. Archived (https://web.archive.org/web/20141016054815/http://marc.info/?l=openssl-announce&m=138747119822324) from the original on 2014-10-16. Retrieved 2013-12-27.
38. "[Cfrg] Dual_EC_DRBG ... [was RE: Requesting removal of CFRG co-chair]" (http://www.ietf.org/mail-archive/web/cfrg/current/msg03651.html). Ietf.org. 2013-12-27. Archived (https://web.archive.org/web/20160818132539/http://www.ietf.org/mail-archive/web/cfrg/current/msg03651.html) from the original on 2016-08-18. Retrieved 2015-12-23.
39. "Aris ADAMANTIADIS: "Dual_Ec_Drbg backdoor: a proof of concept" 31 Dec 2013" (http://blog.0xbadc0de.be/archives/155). 31 December 2013. Archived (https://web.archive.org/web/20141217102434/http://blog.0xbadc0de.be/archives/155) from the original on 17 December 2014. Retrieved 2 January 2014.
40. "*The Many Flaws of Dual_EC_DRBG*" (https://blog.cryptographyengineering.com/2013/09/18/the-many-flaws-of-dualecdrbg/). 18 September 2013. Archived (https://web.archive.org/web/20160820174502/http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html) from the original on 2016-08-20. Retrieved 2016-11-20.
41. Green, Matthew (2015-01-14). "A Few Thoughts on Cryptographic Engineering: Hopefully the last post I'll ever write on Dual EC DRBG" (http://blog.cryptographyengineering.com/2015/01/hopefully-last-post-ill-ever-write-on.html). Blog.cryptographyengineering.com. Archived (https://web.archive.org/web/20151228051108/http://blog.cryptographyengineering.com/2015/01/hopefully-last-post-ill-ever-write-on.html) from the original on 2015-12-28. Retrieved 2015-12-23.
42. Steve Marquess. "Secure or Compliant, Pick One" (https://web.archive.org/web/20131227190128/http://veridicalsystems.com/blog/secure-or-compliant-pick-one/). Archived from the original (http://veridicalsystems.com/blog/secure-or-compliant-pick-one/) on 2013-12-27.
43. "We don't enable backdoors in our crypto products, RSA tells customers" (https://arstechnica.com/security/2013/09/we-dont-enable-backdoors-in-our-crypto-products-rsa-tells-customers/). *Ars Technica*. 2013-09-20. Archived (https://web.archive.org/web/20141012130722/http://arstechnica.com/security/2013/09/we-dont-enable-backdoors-in-our-crypto-products-rsa-tells-customers/) from the original on 2014-10-12. Retrieved 2017-06-14.

44. "Dual_EC_DRBG Added to Windows Vista – Schneier on Security" (https://www.schneier.com/blog/archives/2007/12/dual_ec_drbg_ad.html). Schneier.com. 2007-12-17. Archived (https://web.archive.org/web/20180610182548/https://www.schneier.com/blog/archives/2007/12/dual_ec_drbg_ad.html) from the original on 2018-06-10. Retrieved 2015-12-23.
45. "CNG Algorithm Identifiers" (http://msdn.microsoft.com/en-us/library/aa375534.aspx). Microsoft Developer Network. Archived (https://web.archive.org/web/20170213185952/https://msdn.microsoft.com/en-us/library/aa375534.aspx) from the original on 2017-02-13. Retrieved 2016-11-19.
46. http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf Archived (https://web.archive.org/web/20130927123145/http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf) 2013-09-27 at the Wayback Machine
47. Perlroth, Nicole (10 September 2013). "Government Announces Steps to Restore Confidence on Encryption Standards" (http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/). *New York Times*. Archived (https://web.archive.org/web/20140712084931/http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/) from the original on 12 July 2014. Retrieved 11 September 2013.
48. Hay, Lily (2013-10-09). "Can You Trust NIST? - IEEE Spectrum" (https://spectrum.ieee.org/can-you-trust-nist). IEEE. Archived (https://web.archive.org/web/20160201095426/https://spectrum.ieee.org/telecom/security/can-you-trust-nist) from the original on 2016-02-01. Retrieved 2015-12-23.
49. "Stop using NSA-influenced code in our products, RSA tells customers" (https://arstechnica.com/security/2013/09/stop-using-nsa-influence-code-in-our-product-rsa-tells-customers/). *Ars Technica*. 2013-09-19. Archived (https://web.archive.org/web/20170607180532/https://arstechnica.com/security/2013/09/stop-using-nsa-influence-code-in-our-product-rsa-tells-customers/) from the original on 2017-06-07. Retrieved 2017-06-14.
50. "$10m NSA contract with security firm RSA led to encryption 'back door' " (https://www.theguardian.com/world/2013/dec/20/nsa-internet-security-rsa-secret-10m-encryption). *Guardian*. 20 December 2013. Archived (https://web.archive.org/web/20140125221745/http://www.theguardian.com/world/2013/dec/20/nsa-internet-security-rsa-secret-10m-encryption) from the original on 25 January 2014. Retrieved 14 December 2016.
51. "wired.com: "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA" (Zetter) 24 Sep 2013" (https://www.wired.com/threatlevel/2013/09/nsa-backdoor/all/). Archived (https://web.archive.org/web/20140201111902/https://www.wired.com/threatlevel/2013/09/nsa-backdoor/all/) from the original on 1 February 2014. Retrieved 6 March 2017.
52. "NIST: "DRBG Validation List" " (http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html). Archived (https://web.archive.org/web/20131229110254/http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html) from the original on 2013-12-29. Retrieved 2013-12-30.
53. "Speeds and Feeds › Secure or Compliant, Pick One" (https://web.archive.org/web/20131227190128/http://veridicalsystems.com/blog/secure-or-compliant-pick-one/). Veridicalsystems.com. Archived from the original (http://veridicalsystems.com/blog/secure-or-compliant-pick-one/) on 2013-12-27. Retrieved 2015-12-23.
54. "Digital Dao: "Evolving Hostilities in the Global Cyber Commons" 24 Jan 2014" (http://jeffreycarr.blogspot.dk/2014/01/blackberry-ltd-nsa-and-encryption.html). Archived (https://web.archive.org/web/20140202112547/http://jeffreycarr.blogspot.dk/2014/01/blackberry-ltd-nsa-and-encryption.html) from the original on 2 February 2014. Retrieved 25 January 2014.
55. Derrick Scholl (December 17, 2015). "Important Announcement about ScreenOS" (http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554). Juniper Networks. Archived (https://web.archive.org/web/20151221171526/http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554) from the original on December 21, 2015. Retrieved December 22, 2015.
56. Green, Matthew (2015-12-22). "On the Juniper backdoor" (http://blog.cryptographyengineering.com/2015/12/on-juniper-backdoor.html). *A Few Thoughts on Cryptographic Engineering*. Archived (https://web.archive.org/web/20160829151720/http://blog.cryptographyengineering.com/2015/12/on-juniper-backdoor.html) from the original on 2016-08-29. Retrieved 23 December 2015.
57. Weinmann, Ralf-Philipp. "Some Analysis of the Backdoored Backdoor" (http://rpw.sh/blog/2015/12/21/the-backdoored-backdoor/). *RPW*. Archived (https://web.archive.org/web/20151222092252/https://rpw.sh/blog/2015/12/21/the-backdoored-backdoor/) from the original on 2015-12-22. Retrieved 2015-12-22.

58. "Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA" (https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/). *Wired*. December 22, 2015. Archived (https://web.archive.org/web/20161114170547/https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/) from the original on November 14, 2016. Retrieved December 22, 2015.
59. Dan Goodin - (December 18, 2015). " "Unauthorized code" in Juniper firewalls decrypts encrypted VPN traffic" (https://arstechnica.com/security/2015/12/unauthorized-code-in-juniper-firewalls-decrypts-encrypted-vpn-traffic/). *Ars Technica*. Archived (https://web.archive.org/web/20151222023311/http://arstechnica.com/security/2015/12/unauthorized-code-in-juniper-firewalls-decrypts-encrypted-vpn-traffic/) from the original on December 22, 2015. Retrieved December 22, 2015.
60. "Spy sting: Few at the Swiss factory knew the mysterious visitors were pulling off a stunning intelligence coup – perhaps the most audacious in the National Security Agency's long war on foreign codes – tribunedigital-baltimoresun" (https://web.archive.org/web/20110827112138/http://articles.baltimoresun.com/1995-12-10/news/1995344001_1_crypto-ag-nsa-headquarters-swiss). Articles.baltimoresun.com. 1995-12-10. Archived from the original (http://articles.baltimoresun.com/1995-12-10/news/1995344001_1_crypto-ag-nsa-headquarters-swiss) on 2011-08-27. Retrieved 2015-12-23.

External links

- NIST SP 800-90A – Recommendation for Random Number Generation Using Deterministic Random Bit Generators (http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf)
- Dual EC DRBG (http://projectbullrun.org/dual-ec/) – Collection of Dual_EC_DRBG information, by Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen.
- On the Practical Exploitability of Dual EC in TLS Implementations (http://dualec.org/) – Key research paper by Stephen Checkoway et al.
- The prevalence of kleptographic attacks on discrete-log based cryptosystems (https://link.springer.com/chapter/10.1007%2FBFb0052241) – Adam L. Young, Moti Yung (1997)
- United States Patent Application Publication *US 2007189527 (https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US2007189527), Brown, Daniel R. L. & Vanstone, Scott A., "Elliptic curve random number generation", assigned to Certicom Corp.* on the Dual_EC_DRBG backdoor, and ways to negate the backdoor.
- Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005 (https://web.archive.org/web/20110525081912/http://www.math.ntnu.no/~kristiag/drafts/dual-ec-drbg-comments.pdf) Kristian Gjøsteen's March 2006 paper concluding that Dual_EC_DRBG is predictable, and therefore insecure.
- A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator (https://link.springer.com/chapter/10.1007%2F978-3-540-74143-5_26) Daniel R. L. Brown and Kristian Gjøsteen's 2007 security analysis of Dual_EC_DRBG. Though at least Brown was aware of the backdoor (from his 2005 patent), the backdoor is not explicitly mentioned. Use of non-backdoored constants and a greater output bit truncation than Dual_EC_DRBG specifies are assumed.
- On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng (http://rump2007.cr.yp.to/15-shumow.pdf) Dan Shumow and Niels Ferguson's presentation, which made the potential backdoor widely known.
- The Many Flaws of Dual_EC_DRBG (http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html) – Matthew Green's simplified explanation of how and why the backdoor works.
- A few more notes on NSA random number generators (http://blog.cryptographyengineering.com/2013/12/a-few-more-notes-on-nsa-random-number.html) – Matthew Green
- Sorry, RSA, I'm just not buying it (https://gist.github.com/0xabad1dea/8101758) – Summary and timeline of Dual_EC_DRBG and public knowledge.
- [Cfrg] Dual_EC_DRBG ... [was RE: Requesting removal of CFRG co-chair] (http://www.ietf.org/mail-archive/web/cfrg/current/msg03651.html) A December 2013 email by Daniel R. L. Brown defending Dual_EC_DRBG and the standard process.

- DUELING OVER DUAL_EC_DRBG: THE CONSEQUENCES OF CORRUPTING A CRYPTOGRAPHIC STANDARDIZATION PROCESS (https://harvardnsj.org/wp-content/uploads/sites/13/2022/06/Vol13Iss2_Kostyuk-Landau_Dual-EC-DRGB.pdf) Kostsyuk and Landau article about international cryptographic community's largely continued trust in NIST despite the Dual EC DRBG.