NSA and Cryptography

Why is Cybersecurity important?


ich durch a
er beleben
was zu eng."

Cemal Kaşıkçı'nın 13.14'te konsololuğa geliş

Cemal Kaşıkçı'nın 13.14'te konsololuğa gelişi

- Security is both offense and defense
- Hack everyone else but protect yourself
- Most bugs are implementation level
- Almost never at the cryptography level
- But this is a talk about cryptography


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Other things

- SELinux
- Ghidra
- Equation Group
- Codebreaker Challenge

CLASSIFICATION GUIDE TITLE/NUMBER: (U//FOUO) PROJECT BULLRUN/2-16

PUBLICATION DATE: 16 June 2010

OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and technical challenges of discovering and successfully exploiting systems of interest within the ever-more integrated and security-focused global communications environment.


B-21


B-211


C-35


C-36


C-37


M-209


BC-38


C-443


C-446


C-52


C-52/30


CX-52


CX-52/30


PEB-61


TC-52


BC-543


CD-55


CD-57


HX-63


H-460


CSE-280

MCC-314


HC-520


HC-530


HC-550


HC-570


HC-590


HC-250


CVX-396


CRM-008


HC-3300


HC-4220


HC-2203


HC-5205


SE-160


SE-660


SE-580

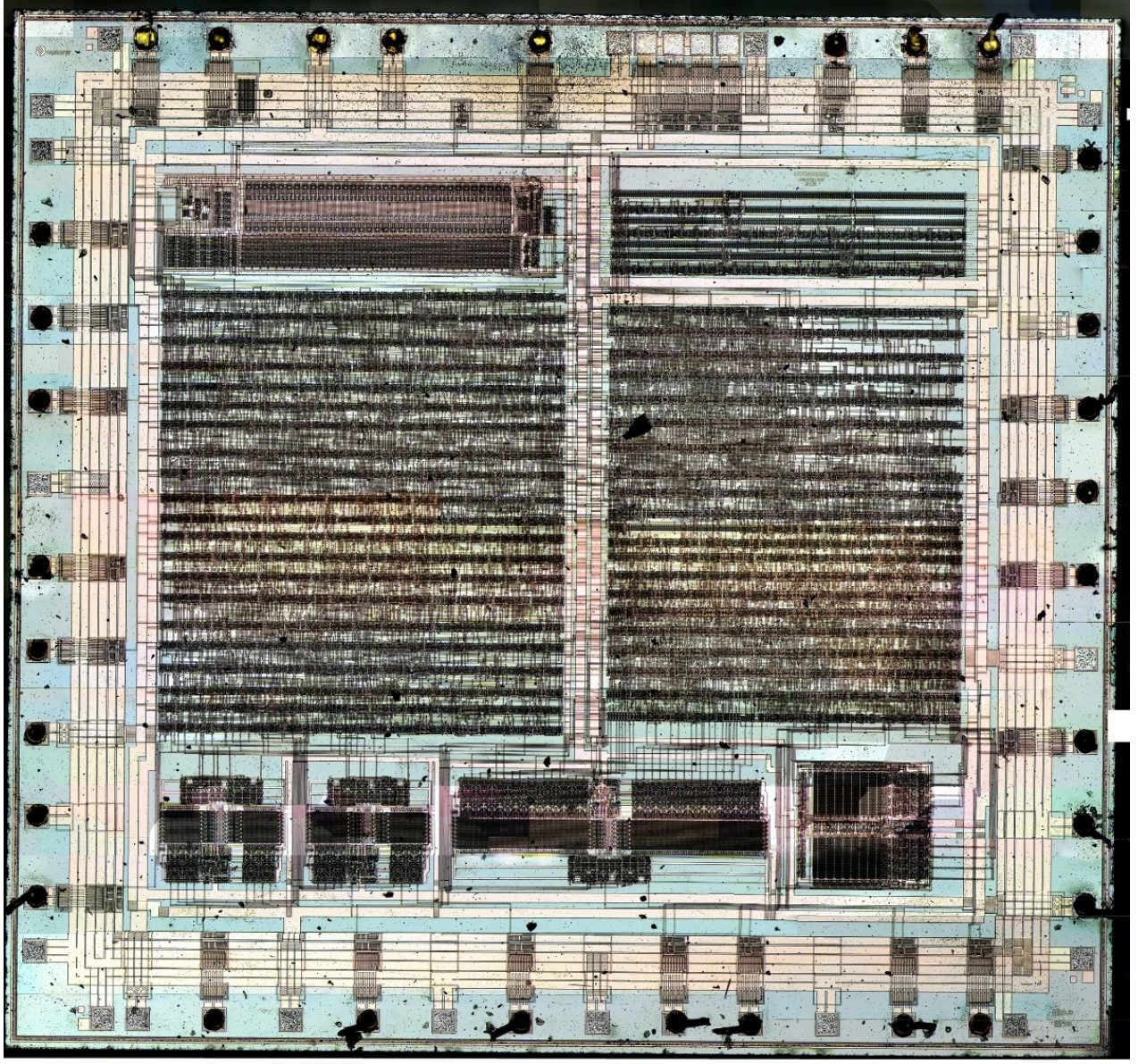

CSE-580


KED-3400


HC-2423

1990s

- Crypto is classified as “munitions”
- Strong crypto is banned from export
- OpenBSD was developed in Canada for this reason
- Netscape has US and international versions with different SSL!
- US: 1024/512 bit RSA/sym
- Intl: 512/40 bit RSA/sym



ADD UNCLE SAM TO YOUR CIRCLE OF FRIENDS AND FAMILY!

Your NATIONAL SECURITY AGENCY

Fort Meade, Maryland

In collaboration with:

U.S. DEPARTMENT OF COMMERCE – NATIONAL INSTITUTE OF TECHNOLOGY AND STANDARDS

FEDERAL BUREAU OF INVESTIGATION

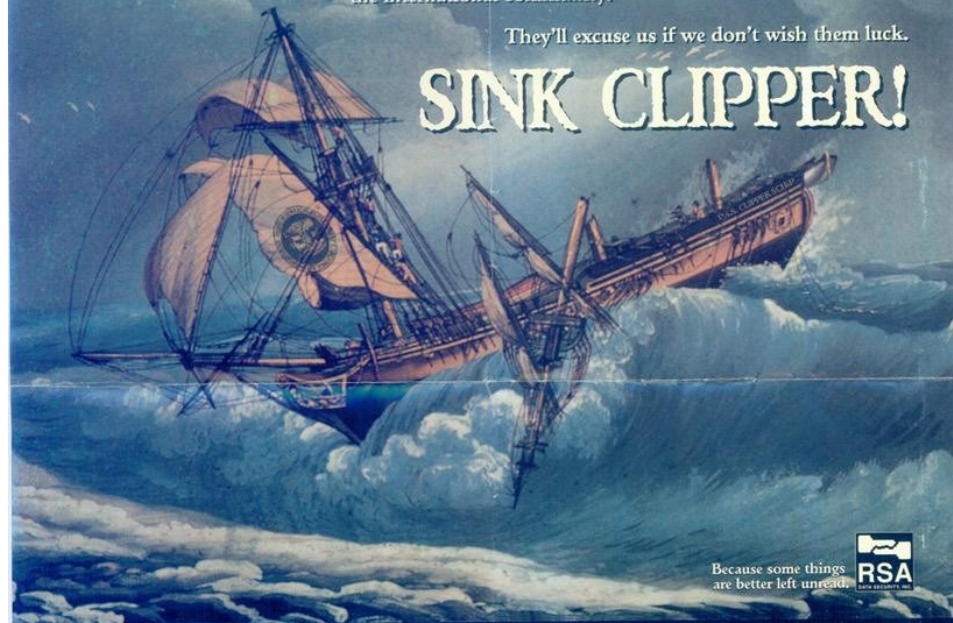
One in a series of marketing campaigns that never made it out of Fort Meade...

On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.

On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.

They'll excuse us if we don't wish them luck.

SINK CLIPPER!



Because some things are better left unread. RSA DATA SECURITY, INC.

What you can do...

BOYCOTT CLIPPER DEVICES AND THE COMPANIES WHICH MAKE THEM EXCLUSIVELY: Don't buy anything with a Clipper Chip in it. Don't buy any product with Big Brother inside. Also, beware of digital signature systems that require the use of a Capstone (Clipper) chip! It is likely that the government will ask you to use Clipper for communications with the IRS, or when doing business with federal agencies. They cannot, as yet, require you to do so. Remember, these people spend YOUR money and work for YOU. You're the shareholder; cast a vote now!

WRITE YOUR REPRESENTATIVES IN WASHINGTON: Since there is nothing quite as powerful as a letter from a constituent, tell your own senators & representative in Washington what you think about the Clipper Proposal and the current restrictions placed upon the export of products which contain robust encryption technology. Tell them that you're seriously concerned about the Clipper Proposal's implications for the personal privacy of U.S. citizens and the global competitiveness of U.S. industry. They may not care much about your privacy in Washington, but they still care about your vote.

ASK FOR RSA BY NAME: Be wary of software and hardware product claims of "security" or "encryption"... many systems contain little more than home-grown scrambling schemes, written by developers with no background in cryptography. Most of them are trivial to break. Find out exactly what kind of security you are getting in your next e-mail, e-forms, cellular devices, operating system or remote access software purchase. Whenever you shop for software that makes claims about security, be sure to ask the sales rep about which algorithms are used inside. Demand the very best in encryption: insist on RSA.

SUPPORT VENDORS THAT SELL PRODUCTS USING REAL RSA ENCRYPTION TECHNOLOGY: Secured software and hardware products that use RSA are available from: Alcatel TITN, ANS CO+RE, Apple, Bankers Trust Company, BLOC Development, Cincinnati Microwave, Cycomm, Cylink, Datamedia, Debtna, Digital Enterprise Solutions, Fischer International, GE Information Services, General Magic, Global Village, Hewlett-Packard, Hilgraeve, Hughes Aircraft, IBM, Lotus, McCaw Cellular, Microsoft, Motorola, National Semiconductor, Newbridge Networks, Northern Telecom, Novell, Oracle, PCSI, Racal Datacom, Retix, Secure Communications Inc, Semaphore; Shana, Storage Tek, SunSoft, Trusted Information Systems, Unisys, WordPerfect and many others. *These companies need to be acknowledged for having the vision and courage to add robust cryptography to their products when the US government has made it as painful as possible. Let them know you approve, and encourage others!*

LEARN MORE: RSA Data Security maintains an extensive library of educational materials on all aspects of the technology. RSA Laboratories' *Frequently Asked Questions About Today's Cryptography* is a great place to start, and it's free.

For a complete list of OEM products that use RSA, call us at (415) 595-8782 or send e-mail to info@rsa.com.

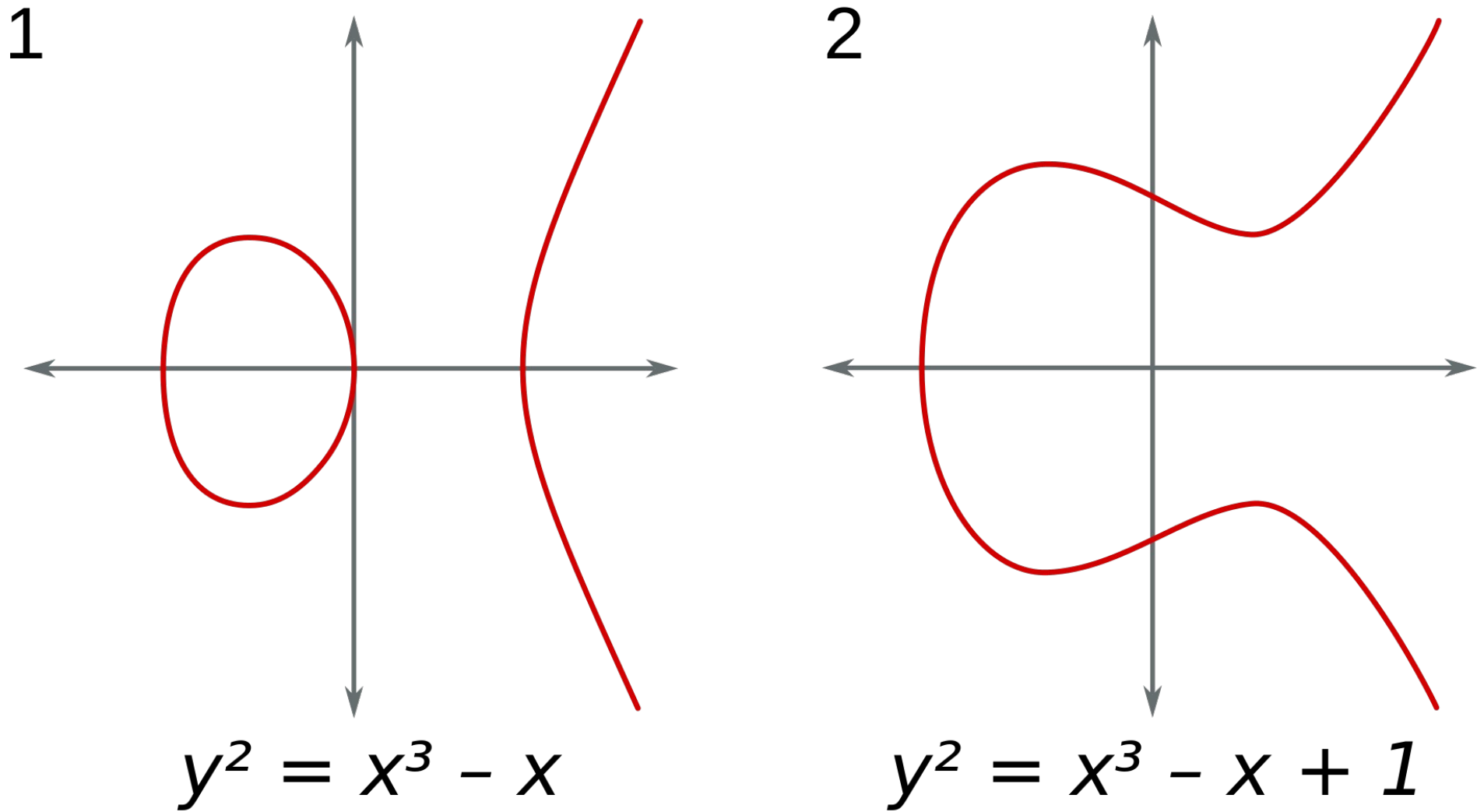
(Many thanks to John Perry Barlow for his suggestions!)

- Junger v. Daley
  - Professor couldn't accept non-US citizens into his class on computer law
- Bernstein v. United States
  - Source code is protected under the first ammendment
- Zimmerman published the PGP source code in a hard cover book
- Still illegal today to export some cryptographic hardware

- Dual EC is a pseudorandom number generator. Soon after its publication it was criticized by experts for its poor design. It is thousands of times slower than alternatives; the numbers that it produces as output are biased, flunking the most basic requirement for a pseudorandom number generator; and, most importantly, it is mathematically guaranteed to have a skeleton key that makes the output entirely predictable to anyone in possession of the key. An honest designer would not have kept the key, but a pseudorandom number generator should not have a skeleton key in the first place.

Elliptic Curves

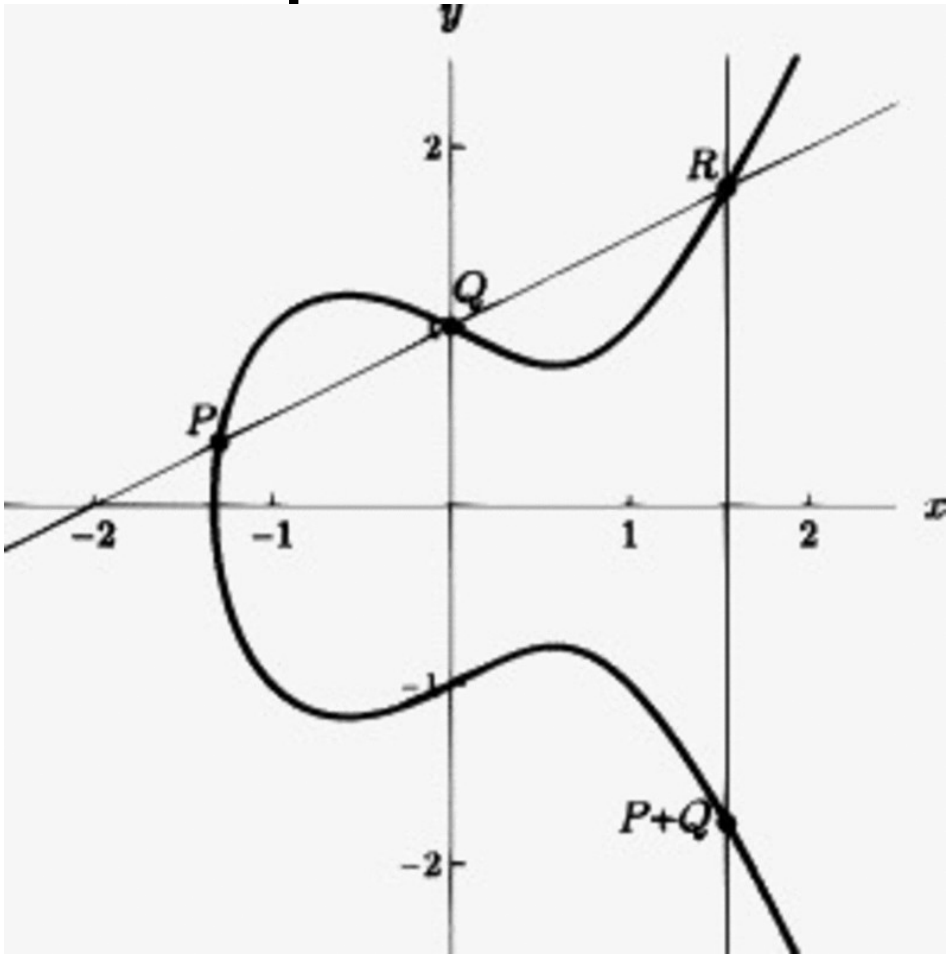
- Define a function over some finite field of the form $y^2 = x^3 + ax + b$
- “weierstrass form”
- Includes a point at infinity


1
2
$y^2 = x^3 - x$
$y^2 = x^3 - x + 1$

Elliptic Curves

- For P,Q points on the curve, define P+Q as -R, where (P,Q,R) are the unique points on the same line

Elliptic Curves



Elliptic Curves

- For P,Q points on the curve, define P+Q as -R, where (P,Q,R) are the unique points on the same line
- Pop quiz! What is P+P?
- What about kP for any integral k?

Elliptic Curves

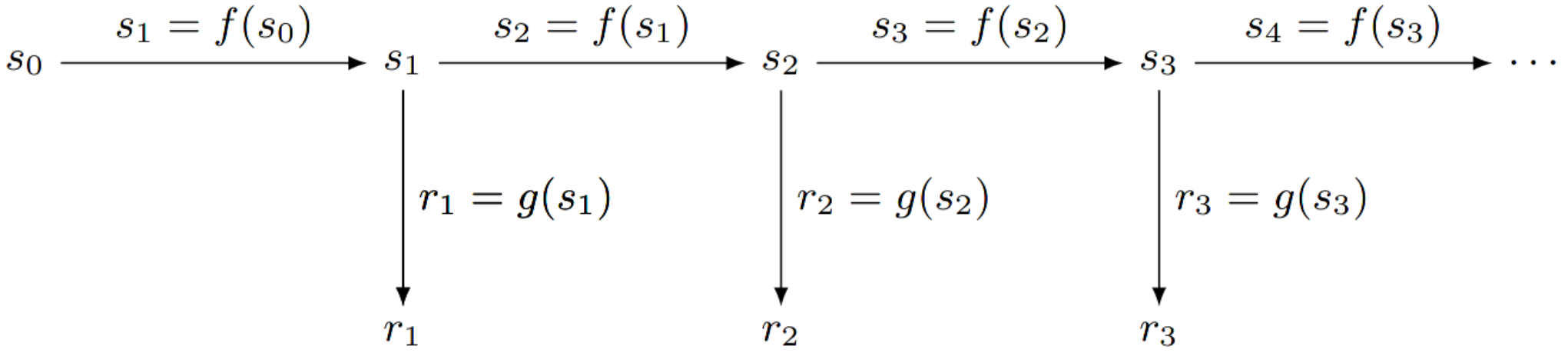
- ECDLP (Elliptic Curve Discrete Log)
- Given P,Q
- Find k such that Q = kP
- I am explicitly not mentioning many details

True randomness

- Actually pretty expensive
- When you do make it you usually don’t want it
- Computer gets it from shaking the mouse, temperature sensors, etc
- Even quantum stuff
- Use TRNG to seed a CSPRNG

CSPRNG

- s0 is a seed from a TRNG
- Knowing s0 can allow you to know all numbers in the future
- Think like how a minecraft world can be uniquely defined by the seed, even though the world is infinitely big


s_0
$s_1 = f(s_0)$
s_1
$s_2 = f(s_1)$
s_2
$s_3 = f(s_2)$
s_3
$s_4 = f(s_3)$
$\cdots$
$r_1 = g(s_1)$
r_1
$r_2 = g(s_2)$
r_2
$r_3 = g(s_3)$
r_3

CSPRNG

- Forward secrecy: Given $r_i = g(s_i)$, hard to compute s_i
- Backward secrecy: Given $s_i = f(s_{i-1})$, hard to compute s_{i-1}
- Pop quiz! Whats an easy way to achieve this?

p = 1157920892103562487626974469494075735300861434152903141955336313088670978539 51

r = 1157920892103562487626974469494075735299969552241357603424222590610685120443 69

b = 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b

Px = 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

Py = 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

Qx = c97445f4 5cdef9f0 d3e05e1e 585fc297 235b82b5 be8ff3ef ca67c598 52018192

Qy = b28ef557 ba31dfcb dd21ac46 e2a91e3c 304f44cb 87058ada 2cb81515 1e610046

- $y^2 = x^3 + 3x + b \pmod{p}$

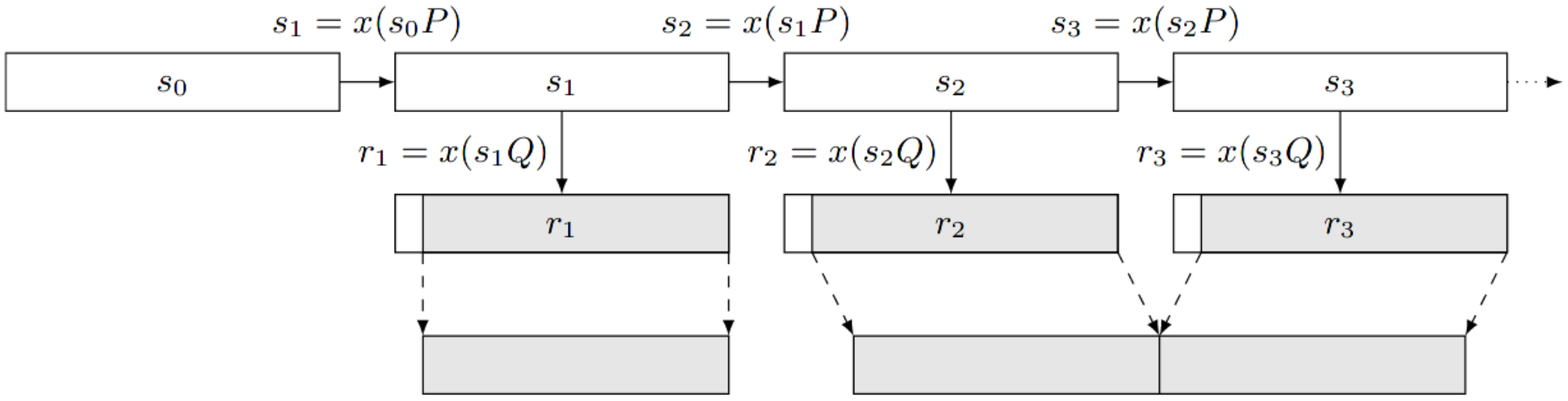


Fig. 5.2. Basic Dual EC algorithm using points P and Q on an elliptic curve.

Dual EC

- Appears to have FS,BS
- Given $s_{i+1} = x(s_iP)$, P, find si
- Given $r_i = x(s_iQ)$, Q, find si
- Implied that these are OWFs from ECDLP

Dual EC

- Suppose P,Q are funny
- P = kQ for some spooky k.
- $kr_1 = k\ x(s_1Q) = s_1\ x(kQ) = s_1x(P) = x(s_1P) = s_2$

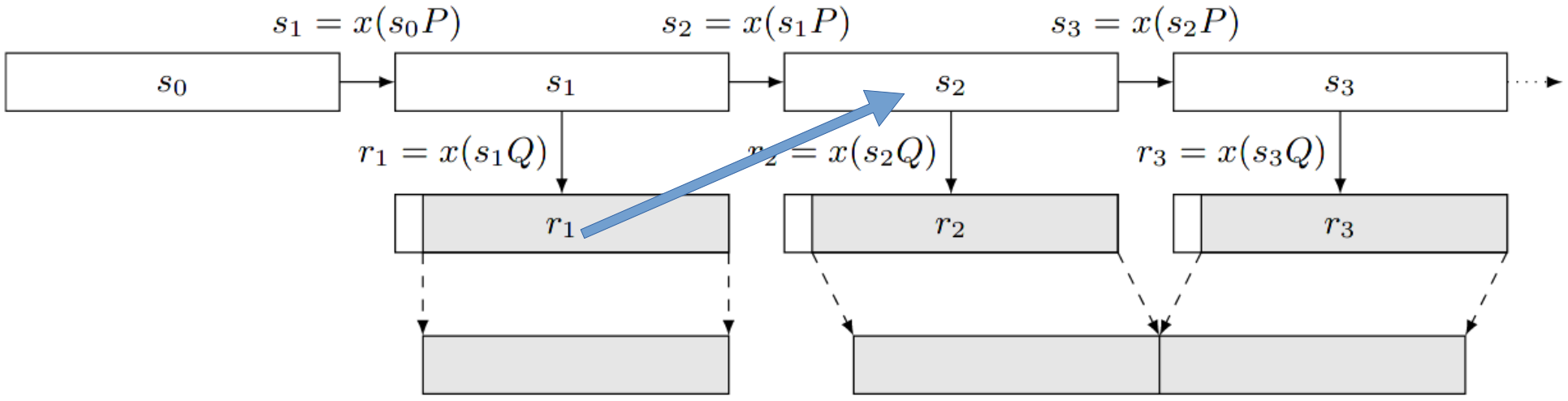


Fig. 5.2. Basic Dual EC algorithm using points P and Q on an elliptic curve.

Dual EC

- Constants like these show up all the time in crypto
- Usually to avoid some specific attacks
- DL usually over a **prime** order group to avoid pollig-hellman
- Maybe some constants fit nicer into x86 registers

Appendix A: (Normative) Application-Specific Constants

A.1 Constants for the Dual_EC_DRBG

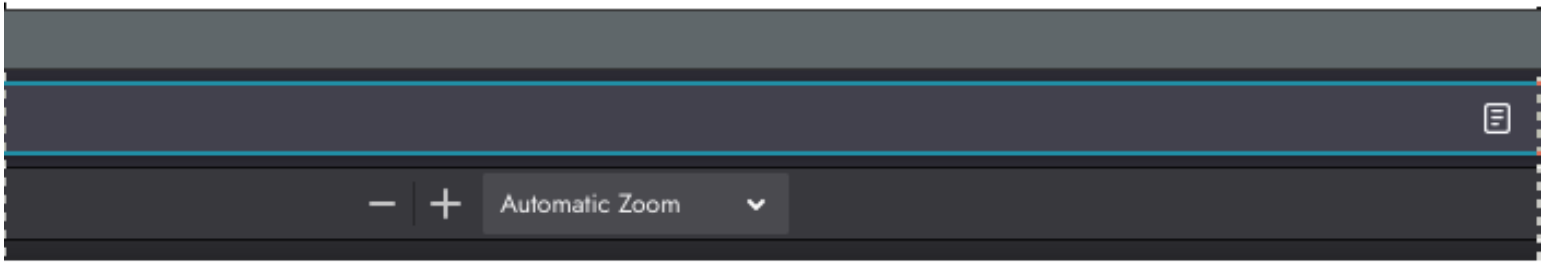
The **Dual_EC_DRBG** requires the specifications of an elliptic curve and two points on the elliptic curve. One of the following NIST approved curves with associated points **shall** be used in applications requiring certification under FIPS 140-2. More details about these curves may be found in FIPS PUB 186-3, the Digital Signature Standard.

A.2 Using Alternative Points in the Dual_EC_DRBG

The security of **Dual_EC_DRBG** requires that the points P and Q be properly generated. To avoid using potentially weak points, the points specified in Appendix A.1 **should** be used. However, an implementation may use different pairs of points, provided that they are *verifiably random*, as evidenced by the use of the procedure specified in Appendix A.2.1 below, and the self-test procedure in Appendix A.2.2. An implementation that uses alternative points generated by this Approved method **shall** have them "hard-wired" into its source code, or hardware, as appropriate, and loaded into the *working_state* at instantiation. To conform to this Recommendation, alternatively generated points **shall** use the procedure given in Appendix A.2.1, and verify their generation using Appendix A.2.2.

Kleptography:
Using Cryptography Against Cryptography

Adam Young* and Moti Yung**



The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone?

Adam Young* and Moti Yung**

Conspiracy

- NSA gives **John Kelsey** Dual EC to include into (NIST SP 800-90A)/(ANSI X9.82) as a fourth CSPRNG
- He forwards questions on it to them and lets them respond

5.2 Bowl, of white porcelain or glazed earthenware.

Various sizes of pot and bowl can be used, but it is recommended that one of the two sizes shown in Annex A, and depicted in Figure A.1, be adopted.

6 Sampling

Sampling shall be carried out in accordance with ISO 1839.

7 Procedure

7.1 Test portion

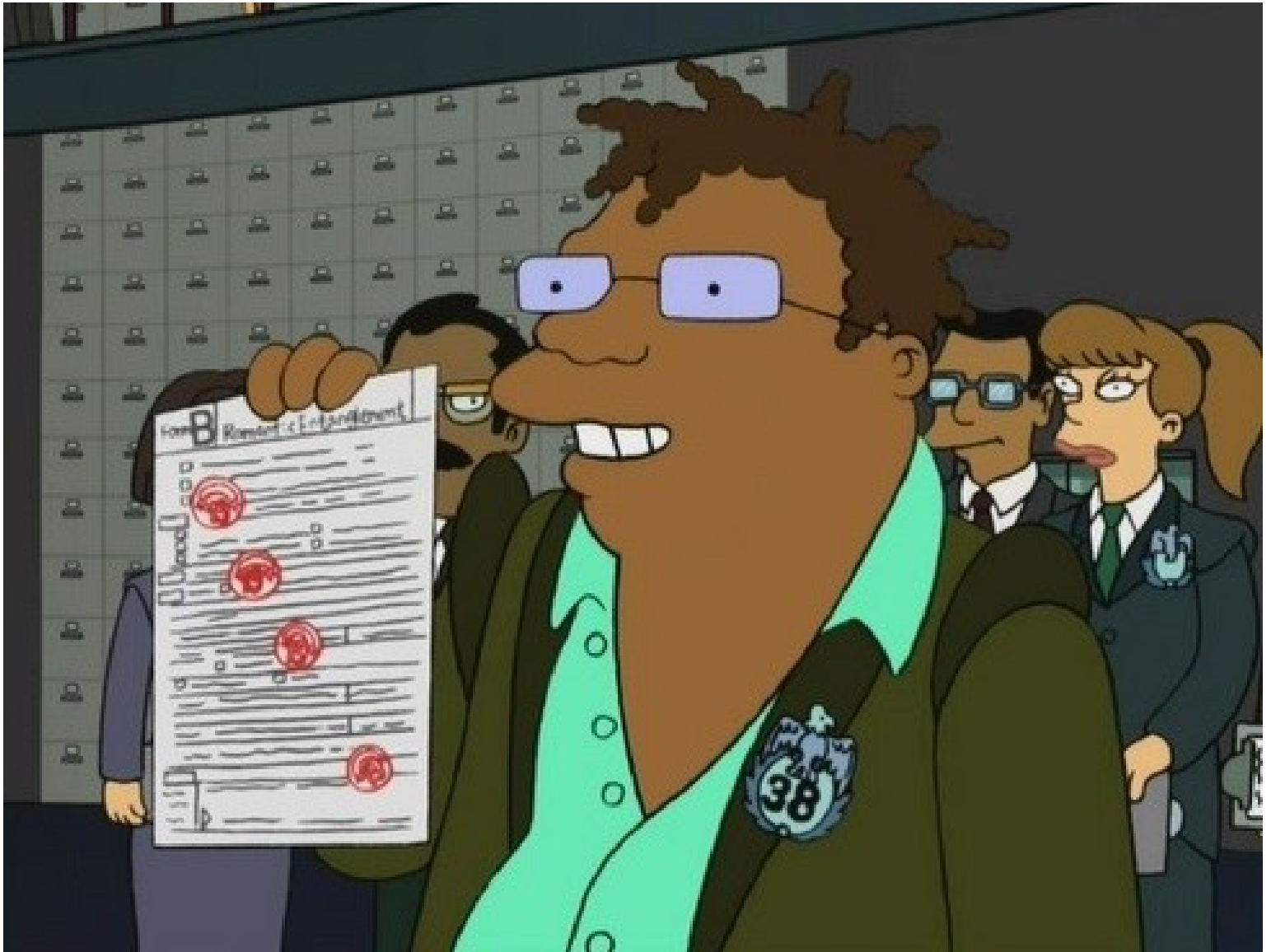
Weigh, to an accuracy of ±2 %, a mass of tea required according to Table 1 and transfer it to the pot (5.1).

7.2 Preparation of liquor

7.2.1 Preparation without milk

Table 1 — Preparation without milk

Type of tea	Test portion	Temperature of water	Brew time
Black	2 g tea per 100 ml 5,6 ± 0,1 g (large pot) 2,8 ± 0,05 g (small pot)	Boiling (approx. 100 °C)	6 min
Green	2 g tea per 100 ml 5,6 ± 0,1 g (large pot) 2,8 ± 0,05 g (small pot)	Boiling (approx. 100 °C)	Leafy type: 5 min Fannings type: 3 min


98

NB[1]	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com-ment[2]	Comment (justification for change) by the NB
US	Whole document		te	The U.S. National Body has reviewed ISO/IEC 2nd CD 18031, N3578. We feel that this document is lacking sufficient depth in many areas and simply is not developed enough to be an ISO standard which encompasses both Non-deterministic and Deterministic Random Bit Generation. We do feel that ANSI X9.82 Random Bit Generation standardization work is much further developed and should be used as the basis for this ISO standard. To make ISO/IEC 18031 consistent with X9.82 would require extensive commenting and revisions. To better progress this standard, the U.S. has instead developed a contribution for ISO that is consistent with ANSI X9.82, but written in ISO format. Furthermore, we believe this contribution will also be complementary to ISO/IEC 19790. We provide this contribution as an attachment, and propose that ISO further develop this contribution as their standard. Additionally, the U.S. recognizes that ANSI X9.82 is not an approved standard and still requires further work. As ANSI X9.82 develops, the U.S. will contribute these changes to ISO.

- The N.S.A. wrote the standard and aggressively pushed it on the international group, privately calling the effort “a challenge in finesse.”

  -NYT

- 2004: NSA pays RSA security $10 million to use Dual EC as the standard CSPRNG in RSA BSAFE
- To get FIPS 140-2 validation, you have to use those P,Q.

Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 3, 2009

E. Rescorla
RTFM, Inc.
M. Salter
National Security Agency

March 02, 2009

Extended Random Values for TLS
draft-rescorla-tls-extended-random-02.txt

Status of this Memo

```
130
131     The United States Department of Defense has requested a TLS mode
132     which allows the use of longer public randomness values for use with
133     high security level cipher suites like those specified in Suite B
134     [I-D.rescorla-tls-suiteb].  The rationale for this as stated by DoD
135     is that the public randomness for each side should be at least twice
136     as long as the security level for cryptographic parity, which makes
137     the 224 bits of randomness provided by the current TLS random values
138     insufficient.
139
```

Margaret Salter

Director AWS Applied Crypto at Amazon

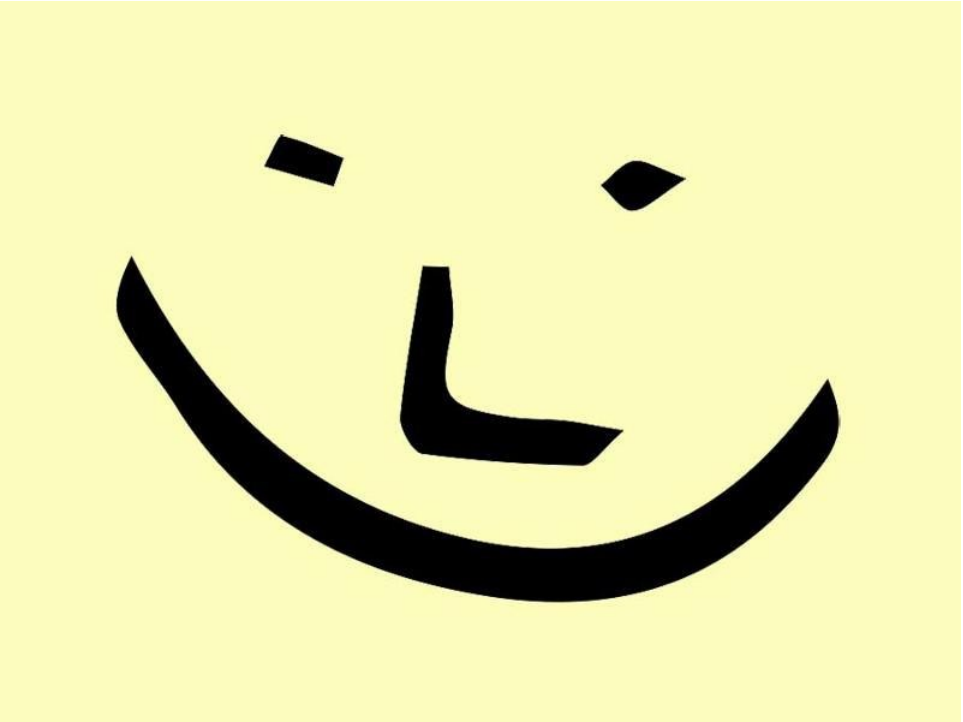
Orlando, Florida, United States · 500+ connections

- Certicom knew as early as January 2005
- Filed a patent of how to backdoor a CSPRNG
- Another patent of protection from a backdoored CSPRNG
- Patent office forwards things like this to respective 3 letter agencies
- NSA recommended against secrecy order

[0018] In yet another aspect, the present invention provides a method of backup functionality for an elliptic curve random number generator, the method comprising the steps of computing an escrow key e upon determination of a point Q of the elliptic curve, whereby $P = eQ$, P being another point of the elliptic curve; instituting an administrator, and having the administrator store the escrow key e; having members with an elliptic curve random number generator send to the administrator, an output r generated before an output value of the generator; the administrator logging the output r for future determination of the state of the generator.

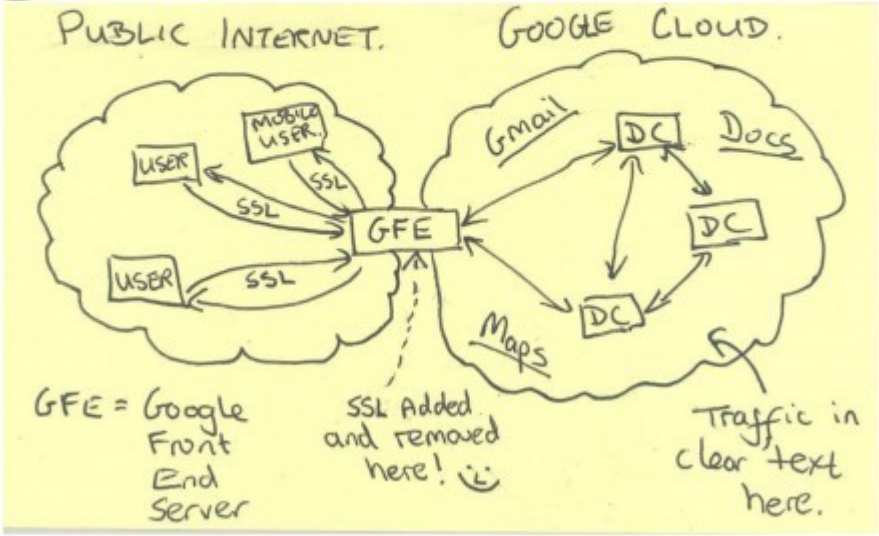
- CRYPTO 2007 Rump session
- Dan Shumow and Niels Ferguson from MSFT detail the possible backdoor
- Internally at NIST, a big deal
- Reported it to NIST in 2005, forwarded it to NSA

- 2013, Snowden leaks
- 2014 paper showed could compromise TLS



TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

NIST Special Publication 800-90

Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Elaine Barker
John Kelsey

Computer Security Division
Inforamtion Technology Laboratory

COMPUTER SECURITY

June 2006

[[Okay, so here's the limit of my competence. Can Don or Dan or one of the NSA guys with some number theory/algebraic geometry background please look this over? Thanks! --JMK]]

[[I'm really blowing smoke here. Would someone with some actual understanding of these attacks please save me from diving off a cliff right here? --JMK]]

Subject: [Fwd: RE: Minding our Ps and Qs in Dual_EC]

Date: Wednesday, October 27, 2004 at 12:09:25 PM Eastern Daylight Time

From: John Kelsey

To: larry.basham@nist.gov

---------- Original Message ----------
Subject: RE: Minding our Ps and Qs in Dual_EC
From: "Don Johnson" <DJohnson@cygnacom.com>
Date: Wed, October 27, 2004 11:42 am
To: "John Kelsey" <john.kelsey@nist.gov>

John,

P = G.
Q is (in essence) the public key for some random private key.

It could also be generated like a(nother) canonical G, but NSA kyboshed this idea, and I was not allowed to publicly discuss it, just in case you may think of going there.

Don B. Johnson

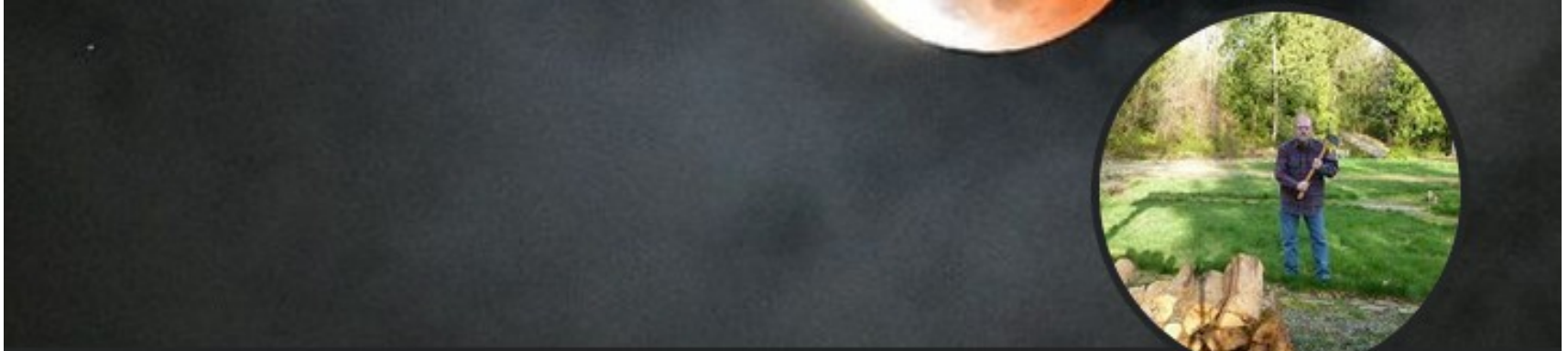
-----Original Message-----
From: John Kelsey [mailto:john.kelsey@nist.gov]
Sent: Wednesday, October 27, 2004 11:17 AM
To: Don Johnson
Subject: Minding our Ps and Qs in Dual_EC

Do you know where Q comes from in Dual_EC_DRBG?

Thanks,

-John

- Don Johnson
- **Debby Wallner**
- Bob Karkoska
- Paul Timmel
- Mike Boyle



Don Johnson

No

Posts About Friends Photos Videos Check-Ins More

Do you know Don?

To see what he shares with friends, send him a friend request.

Intro

Former Head Snitch at **NSA - National Security Agency**

Posts

Mike Boyle is the Co-Lead for NSA's Center for Cybersecurity Standards. He creates and resources NSA's strategy for standards development, focusing on secure, interoperable products that protect US National Security Systems. He has a long history of leading efforts with government and industry partners to tackle difficult cybersecurity problems. Boyle began his career as a cryptomathematician at NSA, using his skills to understand how good cryptography can fail in implementation and working with industry to ensure that products purchased by the US government avoid those pitfalls. His focus has evolved to include secure network protocols. He is active in several open standards efforts dedicated to their development. He is active in DoD and NSA efforts to drive the use of secure, interoperable standards.

- As late as 2016, Dual EC was still being used in the wild
- Juniper supposedly were using it in a secure way
- But then the code was buggy, so it was just vanilla Dual EC

(TS//SI//REL) **TUNDRA** -- Electronic codebooks, such as the Advanced Encryption Standard, are both widely used and difficult to attack cryptanalytically. NSA has only a handful of in-house techniques. The TUNDRA project investigated a potentially new technique -- the Tau statistic -- to determine its usefulness in codebook analysis. This project was supported by [redacted] of R21.

Simon and Speck

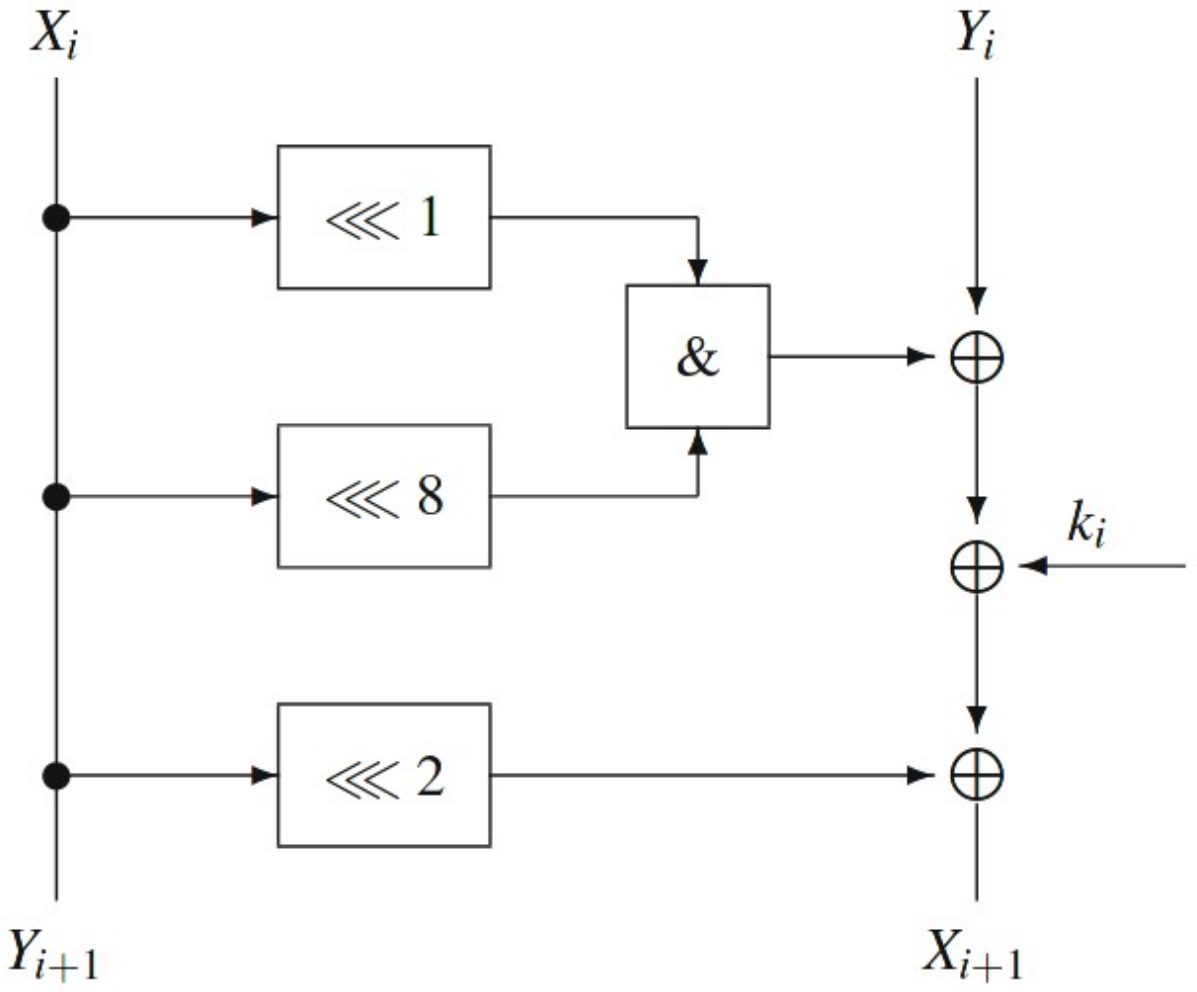


Fig. 4.1 One round of Simon (without the final swap operation)

SIMON and SPECK: Block Ciphers for the Internet of Things*

Ray Beaulieu Douglas Shors Jason Smith
Stefan Treatman-Clark Bryan Weeks Louis Wingers

National Security Agency
9800 Savage Road, Fort Meade, MD, 20755, USA

Design Rationale

- Whats the point? What are you securing against? What do you consider an attack?
- NSA provided no rationale
- Cryptanalysis was quickly published by multiple sources

- A block cipher for IoT
- “constrained enviroments where AES may not be suitable”
- 3x faster than AES

1 Introduction

Biologists make a distinction between specialist species, which occupy narrow ecological niches, and generalists, which can survive in a broader variety of environmental conditions. Specialists include Kirtland's warbler, a bird that only nests in 5–20 year-old jack pine forests, and the koala, which feeds (almost) exclusively on eucalyptus leaves. Generalists such as the American crow and the coyote are able to adapt to a variety of different environments. In a stable world, it's a good strategy to specialize, but when conditions change rapidly, specialists don't always fare so well.

We would argue that what's needed in the Internet of Things (IoT) era is not more Kirtland's warblers and koalas, as wonderful as such animals may be, but crows and coyotes. An animal that eats only eucalyptus leaves, even if it outcompetes the koala, will never become widely distributed. Similarly, a block cipher highly optimized for performance on a particular microcontroller will likely be outcompeted on other platforms, and could be of very limited utility in 15 years when its target platform is obsolete.

- Lets not get too deep into the cryptanalysis
- Basically it sucks

- They wanted it standardized!?
- Many meetings took place over many months in many countries
- Mexico City
- Malaysia
- India
- Tampa
- Abu Dhabi
- New Zealand
- Berlin
- Wuhan

- “Not mentioned in the meeting summary is a discussion that was held about past involvement of the NSA in sabotaging cryptographic standards, e.g., Dual-EC. One of the NSA experts, **Debby Wallner**, who was also involved in the standardization of Dual-EC, referred to it as the “elephant-in-the-room” and claimed that they had apologized for it and that it was time to move on. [9]”

First, I'd like to say that the NSA has done quite extensive work in muddying the waters, arguing that Simon & Speck are secure and that all objections are political. This is not true, as I will now show with examples. The bottom line is that there are still many open questions about their security, questions that the NSA has, on multiple occasions, refused to answer.

More than once they argued in a meeting that the cryptanalysis for the ciphers has been stabilized (i.e., that attacks will not improve) just to be proved wrong in the next meeting (their answer: "well, _now_ it has fully stabilized", which was again proven wrong in the next meeting). One of them even had a bet with Tanja Lange that no attack on either Simon or Speck would be extended by 3 rounds or more in the upcoming year. He lost this bet. They were very uncooperative, and made it a point to let us know that they will not be providing more information about the algorithms.

Tanja Lange
@hyperelliptic

I'm still waiting for email confirmation, but for the public record: I've made a bet with Louis Wingers (NSA) during ISO meeting on April 11

10:43 PM · Apr 13, 2016 · Twitter Web Client

1 Retweet **13** Likes

Tanja Lange @hyperelliptic · Apr 13, 2016
Replying to @hyperelliptic
Amount: 300 USD. I win if >=3 more rounds of Simon or Speck (any proposed parameters) broken by anybody; attack must be online by 2017-04-11

1 4 6

4. Lies - this is the most troubling part. The NSA lies to the public (including the American people) on official documents. I already wrote that the choice for the exact number of rounds is only motivated through some hand waving. This makes it hard to tell what the real security margin is. But even if you interpret the hand waving conservatively, the math results in much smaller security margins than what is claimed. I gave a rump session talk about this in Crypto 2017 which you can view here [3]. The talk focuses on Simon but the story for Speck is similar and results in security margins of 15.6%, 15.6%, and 14.7% for Speck128 with key sizes 128, 192, and 256, respectively. According to the NSA, that is, and only if you accept the claim that attacks have stabilized.

   the choice for the number of rounds was heavily discussed in the ISO meeting in Berlin about 6 months ago. When confronted with this question, the NSA answered (again) that they will not be providing further information, added that anyone with a decent level of English would immediately understand what they meant, and called me an incompetent cryptographer. Nevertheless, a few months after the meeting they updated the so-called design rationale and added a footnote that reads:

All of this was known to the people in the room when ISO made its decision to reject Simon and Speck (after deliberating about this for more than 3 years. Not because there were disagreements but because we wanted to give the NSA a fair chance). These people also got a first hand impression of how poorly the people the NSA sent fare with _technical_ questions, basically refusing to answer all, and throwing tantrums instead. And then, the ISO people also saw another thing. During the discussions I asked the NSA two non-technical questions (from a crypto point of view. These are technical questions from a standardization point of view):

- Q: You claim that third party analysis is indicative of the algorithm's real security. Were you aware of all these results when you published the algorithms, or are any of them better than what you knew of?
- A: I refuse to answer that
- Q: Are you aware of any cryptanalytic results better than those already found by academia?
- A: I refuse to answer that either.

“I don’t trust the designers,” Israeli delegate Orr Dunkelman, a computer science professor at the University of Haifa, told Reuters, citing Snowden’s papers. “There are quite a lot of people in NSA who think their job is to subvert standards. My job is to secure standards.”

List: linux-crypto-vger
Subject: [RFC PATCH 0/9] crypto: HPolyC support
From: Eric Biggers <ebiggers () kernel ! org>
Date: 2018-08-06 22:32:51
Message-ID: 20180806223300.113891-1-ebiggers () kernel ! org
[Download RAW message or body]

From: Eric Biggers <ebiggers@google.com>

Hi all,

(Please note that this patchset is a true RFC, i.e. we're not ready for
it to be merged quite yet!)

It was officially decided to *not* allow Android devices to use Speck
encryption [1]. We've been working to find an alternative way to bring
storage encryption to entry-level Android devices like the inexpensive
"Android Go" devices sold in developing countries. Unfortunately, often
these devices still ship with no encryption, since for cost reasons they
have to use older CPUs like ARM Cortex-A7; and these CPUs lack the ARMv8
Cryptography Extensions, making AES-XTS much too slow.

author	Jason A. Donenfeld <Jason@zx2c4.com> 2018-08-07 08:22:25 +0200
committer	Herbert Xu <herbert@gondor.apana.org.au> 2018-09-04 11:35:03 +0800
commit	578bdaabd015b9b164842c3e8ace9802f38e7ecc (patch)
tree	6a1b6134e2377490812b7aa27620f2330e94576e
parent	9dbe3072c6b1f28000961e34497237d0e3d13318 (diff)
download	cryptodev-2.6-578bdaabd015b9b164842c3e8ace9802f38e7ecc.tar.gz

crypto: speck - remove Speck

These are unused, undesired, and have never actually been used by anybody. The original authors of this code have changed their mind about its inclusion. While originally proposed for disk encryption on low-end devices, the idea was discarded [1] in favor of something else before that could really get going. Therefore, this patch removes Speck.

- Ray Beaulieu
- Douglas Shors
- Jason Smith
- Stefan Treatman-Clark
- Bryan Weeks
- Louis Wingers

Beaulieu Ray

Applied Research Mathematician at US Department of Defense

San Diego County, California, United States · 30 connections

Post Quantum Crypto

Where we are today

- Quantum computers are an incoming threat
- Can break certain hardness assumptions used
- (if you can build one)
- Integer factorization, discrete log, and variants
- But not all! Some are believed secure
- Hash functions, lattices, block ciphers, oil-and-vinegear

⟨quantum|gov⟩

pqc-...@list.nist.gov <pqc-forum@list.nist.gov> ☆

Hi Dan,

This quote is nuts.

Apparently everyone but you understands the state of the science, and is willing to accept new results as they happen.

Stop propagandizing.

Best,
--Daniel Apon, NIST PQC.

On Saturday, June 19, 2021 at 11:35:29 AM UTC-4 D. J. Bernstein wrote:

Some 3rd round Finalists Encryption

- Decoding hardness: **Classical McEliece**, BIKE, HQC
- NTRU-like: **NTRU**, NTRU-prime
- LWE (or variants):**Crystals-Kyber**, **Saber**, FrodoKEM
- Isogeny: SIKE

Some 3rd round Finalists Signatures

- LWE (or variants): **Crystals-Dilithium**
- NTRU-like: **FALCON**
- Multivariate: **Rainbow**, GeMSS
- Hash: SPHINCS+
- Zero Knowledge: Picnic
- The signature is a NIZKPOK of the secret key!
- Hash function and block cipher assumptions

Q: When will NSA select a NIST-approved algorithm?
A: NIST has indicated that it will likely standardize multiple post-quantum algorithms at multiple security levels from their Round 3 finalists, to include a lattice-based algorithm for confidentiality and a lattice-based signature. To enable interoperability within NSS, NSA anticipates using these lattice-based standards, likely at one of the higher security levels. The precise choice will be announced after NIST makes its selections. There is usually a significant period of time between a NIST selection announcement and publication of the final standard. NSA may announce its choice(s) before the final NIST standard is published in order to help the NSS community plan for implementation. Official deployment will not begin until the final standard is published; certification and validation processes are in place; and a robust plan for post-quantum cryptography acquisition, transition and interoperability is established. It is likely that commercial vendors will be offering some support before the process is complete. NSA has full confidence in the NIST Post-Quantum Cryptography Standardization process.

NSA's Cybersecurity Perspective on Post-Quantum Cryptography Algorithms

Lattice-based cryptography:

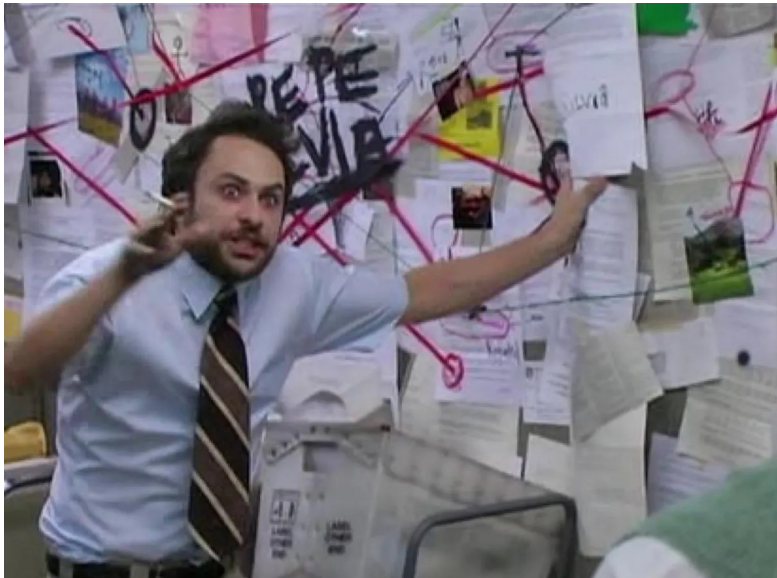
Lattice-based cryptography derives its security from the related problems of finding a short vector in a lattice or finding a lattice vector that is close to a target vector not in the lattice. These systems are fairly well-studied in cryptologic literature, and analysis suggests that these systems can be secure when well-parameterized. We agree with the NIST assessment, documented in NISTIR 8309: Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, that these are among the most efficient post-quantum designs. Based on their history of analysis and implementation efforts, NSA CSD expects that a NIST-candidate lattice-based signature and a NIST-candidate lattice-based key encapsulation mechanism will be approved for NSS.

Hash-based signatures:

Hash-based signatures are based on the well-understood security of inverting a hash function. These systems are also fairly well-studied in cryptologic literature, and analysis suggests that these systems can be secure when well-parameterized. However, the stateful versions have a limited number of allowable signatures per public key and require the signer to maintain an internal state. Because of this, they are not suitable for all applications. NSA CSD expects that the stateful signatures LMS and XMSS will be standardized by NIST in NIST SP 800-208 and approved for NSS solutions for certain niche applications where maintaining state is not a problem.

At the present time, NSA CSD does not anticipate the need to approve other post-quantum cryptographic technologies for NSS usage, but recognizes circumstances could change going forward. A variety of factors—including confidence in security and performance, interoperability, systems engineering, budgeting, procurement, and other requirements—could affect such decisions.

- Reverse Psychology?
- Reverse Reverse Psychology?
- Reverse Reverse Reverse Psychology?
- Reverse Reverse Reverse Reverse Psychology?
- etc



My best guesses Encryption

- NSA also wants to secure themselves from quantum adversies
- Codes seem more secure to me than lattices only because I don't understand lattices
- I don't understand codes either. But I don't know that I don't know that
- Maybe some future magical lattice theorem seems more likely

My best guesses Signatures

- SPHINCS+ only relies on hash function assumptions
- Maybe can be configured to be misused?
- MD5 is still in coreutils. Is it on your system?
- SPHINCS+ relies on AES-NI and SHA256 in AVX2

Closing Thoughts

- Whos winning? Cryptographers? NSA?
- Hard to say
- I gave you lots of names of people


What w
Revie
Docu
Bette

The Moral Character of Cryptographic Work*

Phillip Rogaway

Department of Computer Science
University of California, Davis, USA
rogaway@cs.ucdavis.edu

December 2015
(minor revisions March 2016)

- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf
- https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/
- https://link.springer.com/content/pdf/10.1007%2F3-540-69053-0_6.pdf
- https://link.springer.com/content/pdf/10.1007%2FBFb0052241.pdf
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-90.pdf
- https://csrc.nist.gov/csrc/media/projects/crypto-standards-development-process/documents/dualec_in_x982_and_sp800-90.pdf
- https://icmconference.org/wp-content/uploads/Y30a-Green.pdf
- https://rump2007.cr.yp.to/15-shumow.pdf
- https://pure.tue.nl/ws/portalfiles/portal/3854147/588733604251427.pdf
- https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation-search?searchMode=validation&productType=-1&algorithm=49&ipp=75&orderBy=ValidationDate&page=1
- https://www.spiegel.de/media/411ee8b9-0001-0014-0000-000000035550/media-35550.pdf
- https://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html
- https://www.nsa.gov/What-We-Do/Cybersecurity/NSAs-Cybersecurity-Perspective-on-Post-Quantum-Cryptography-Algorithms/
- https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF
- https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF
- https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf
- https://projectbullrun.org/dual-ec/documents/11336814.pdf
- https://projectbullrun.org/dual-ec/documents/60644982.pdf
- https://csrc.nist.gov/projects/random-bit-generation#RNG%20WSD
- https://eprint.iacr.org/2006/190
- https://www.uspto.gov/web/offices/pac/mpep/s115.html
- https://github.com/matthewdgreen/nistfoia
- https://datatracker.ietf.org/doc/html/draft-hoffman-tls-additional-random-ext-01
- https://datatracker.ietf.org/doc/html/draft-solinas-tls-additional-prf-input-01
- https://csrc.nist.gov/csrc/media/events/lightweight-cryptography-workshop-2015/documents/papers/session1-shors-paper.pdf
- https://www.spinics.net/lists/linux-crypto/msg33291.html
- https://git.kernel.org/pub/scm/linux/kernel/git/herbert/cryptodev-2.6.git/commit/?anzwix=1&id=578bdaabd015b9b164842c3e8ace9802f38e7ecc