CSE107: Intro to Modern Cryptography

https://cseweb.ucsd.edu/classes/sp22/cse107-a/

Emmanuel Thomé

June 2, 2022

Lecture 19

Elliptic curves

Definition

The group law

In protocols

Demystifying (perhaps)

Public-key cryptography is already quite complex, and having a good grasp of concepts requires some work.

People are sometimes afraid of elliptic curves. They should not. Elliptic curves are just groups. Moreover, they're easy to deal with

Plan

Definition

The group law

In protocols

Back to lecture 9

$\sim$ 5 weeks ago, we discussed this example:

Fact

The set of pairs (x, y) of rational numbers such that $x^2 + y^2 = 1$ is a group under the operation:

$$(c_1, s_1) \cdot (c_2, s_2) = (c_1 c_2 - s_1 s_2, c_1 s_2 + c_2 s_1)$$

- the identity element is $\mathbf{id} = (1, 0)$.
- the inverse of (c, s) is $(c, -s)$.

Examples of elements: $(3/5, 4/5)$, or $(5/13, 12/13)$ (Pythagorean triples).

Algebraic groups

The previous example is an easy case of an algebraic group.

Another example: 2×2 matrices with determinant 1 over $\mathbb{Z}$. These are just quadruples $(a, b, c, d) \in \mathbb{Z}^4$ with $ad - bc = 1$. Exercise: figure out the group law (multiplication and inversion).

Elliptic curves are another example.

Algebraic groups

Definition (Algebraic groups)

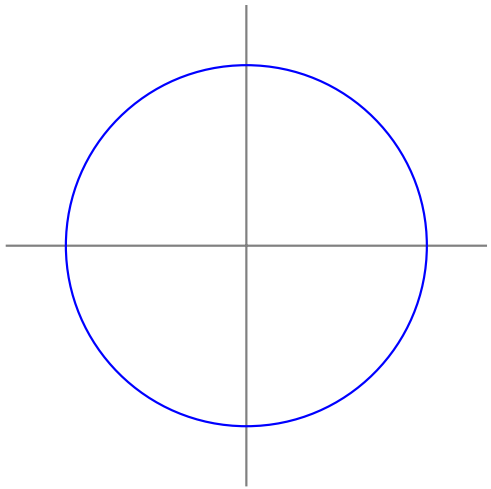
An algebraic group is:

- A set of points with coordinates in a field;
- which all satisfy one or several defining equations;
- and sometimes we can make a group out of this, with completely explicit formulas.

If coordinates are taken in a finite field, then we're talking of finite sets of solutions.

Examples

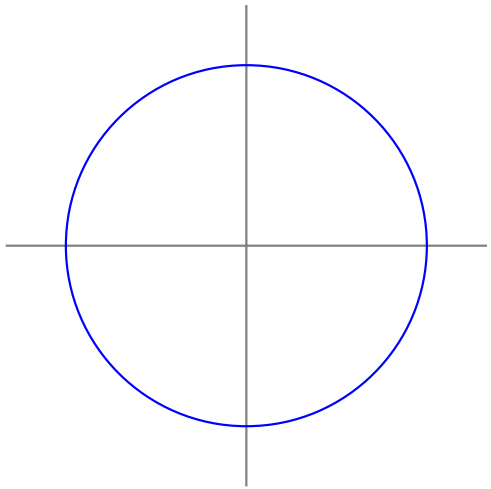
We can think of sets of solutions over the reals:



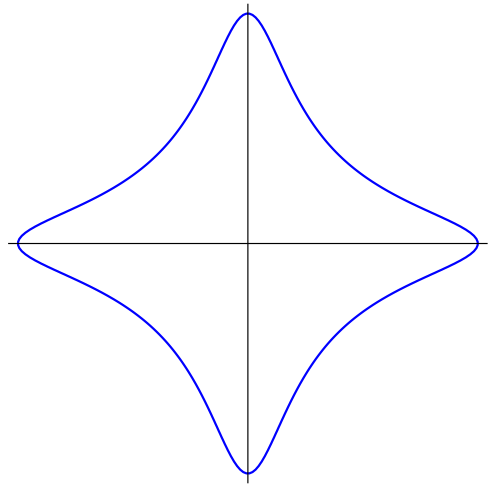
$x^2 + y^2 = 1$

Examples

We can think of sets of solutions over the reals:



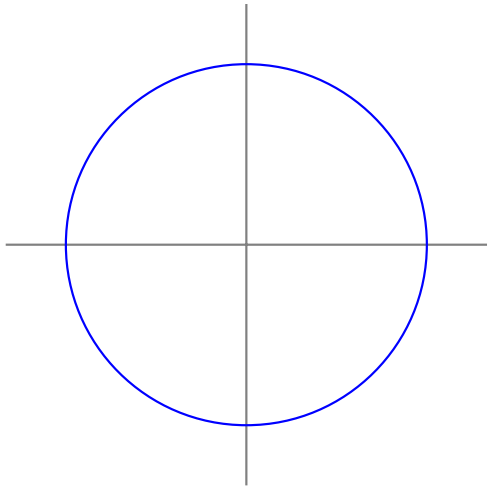
$x^2 + y^2 = 1$



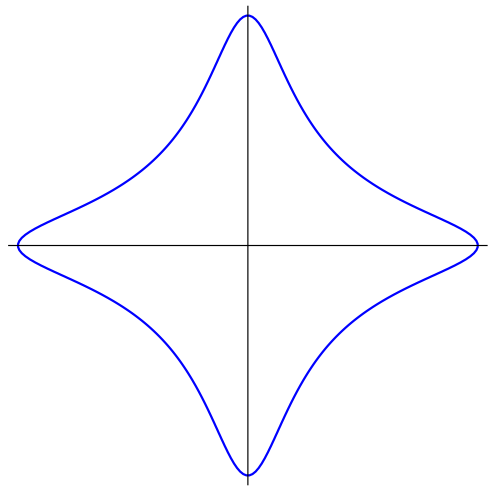
$x^2 + y^2 = 1 + 30x^2y^2$

Examples

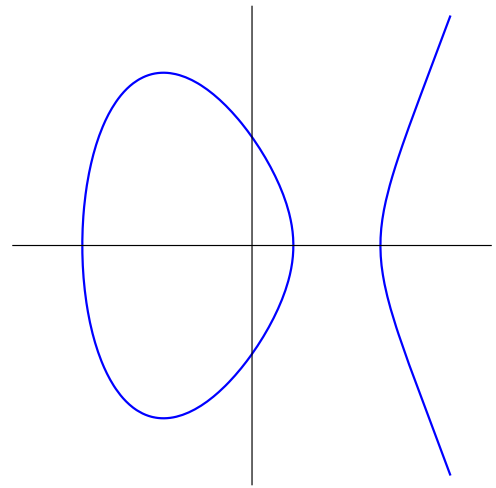
We can think of sets of solutions over the reals:



$x^2 + y^2 = 1$



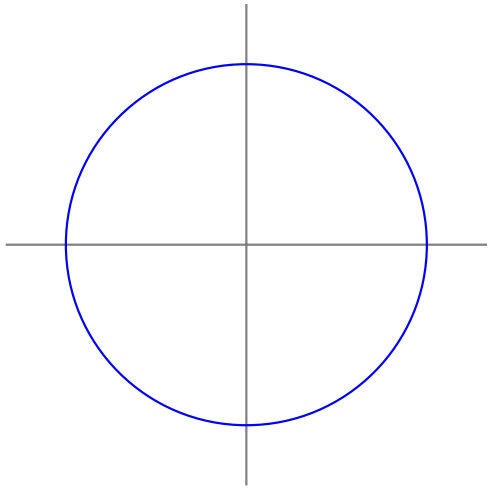
$x^2 + y^2 = 1 + 30x^2y^2$



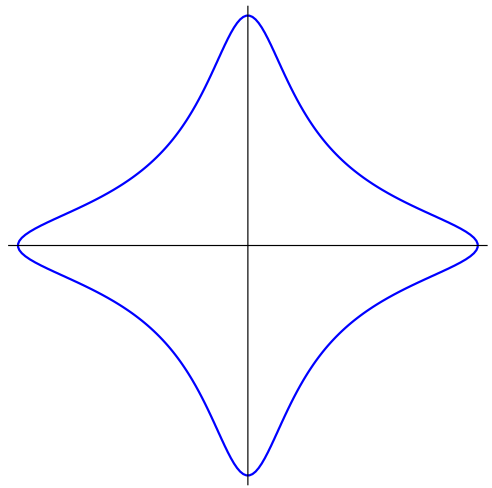
$y^2 = x^3 - 4x + 2$

Examples

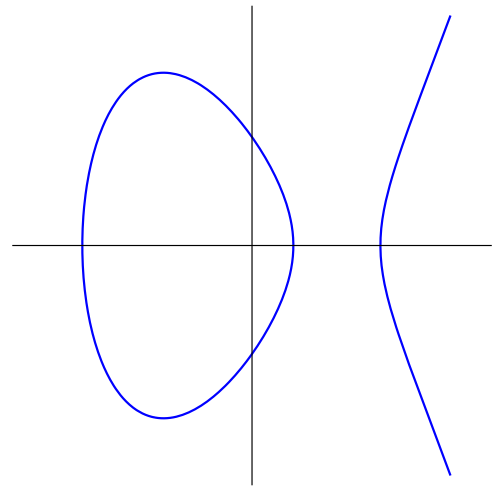
We can think of sets of solutions over the reals:



$x^2 + y^2 = 1$

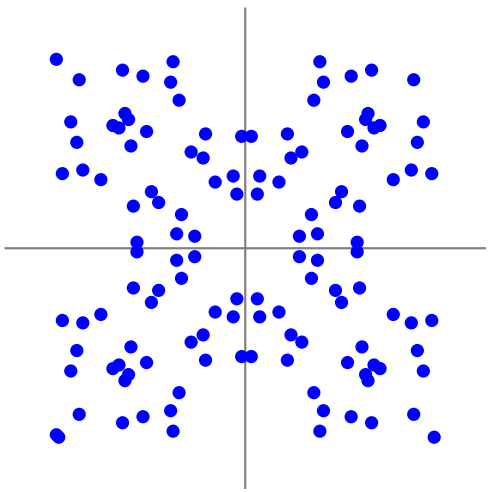


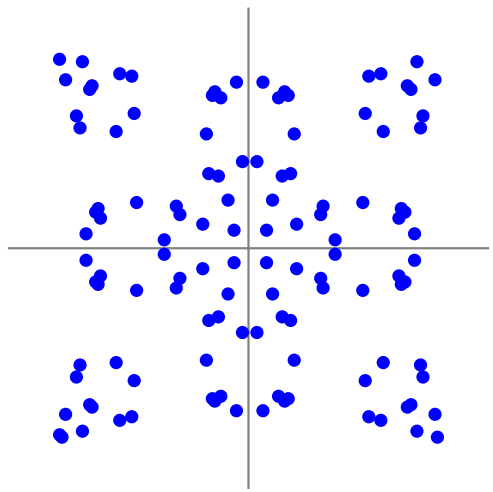
$x^2 + y^2 = 1 + 30x^2y^2$

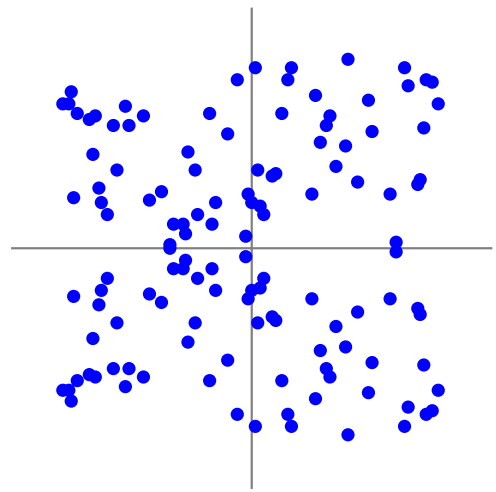


$y^2 = x^3 - 4x + 2$

It looks somewhat different on a finite field (here $\mathbb{Z}_{127}$)







Computing with curves

The two latter curves are examples of elliptic curves:

- $x^2 + y^2 = 1 + 30x^2y^2$
- $y^2 = x^3 - 4x + 2$

They are different curves! Over a finite field, we can define many curve equations and they are generally distinct.

The most important thing about the groups we want to deal with are:

- Elements are points, with coordinates.
- We deal with them with simple equations.

An example elliptic curve: Ed25519

This curve is currently being standardized for widespread use (it is part of FIPS 186-5).

Two aspects:

- What is the curve exactly? How do we do operations?
- How do we use it in a crypto protocol?

Ed25519 is an Edwards curve

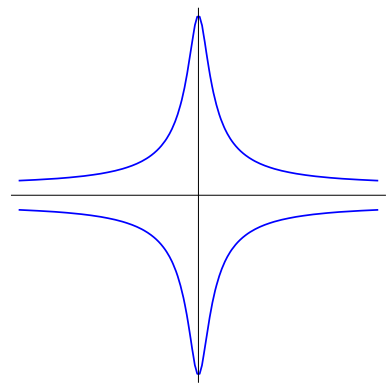
Ed25519 is one way to look at a curve otherwise known as Curve25519.

The curve is defined over the field $\mathbb{Z}_p$ with $p = 2^{255} - 19$. This means that all operations that we do will eventually boil down to operations in $\mathbb{Z}_p$.

The defining equation is

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

for a fixed constant $d = 1/121666 - 1$.



How many points?

Nontrivial fact

An elliptic curve over a finite field $\mathbb{Z}_p$ has a number of points $\#E$ such that

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}.$$

In other words: p being a 255-bit prime, $\#E$ is also a 255-bit number quite close to p.

Ed25519 / Curve25519 is chosen so that $\#E = 8\ell$ with ℓ a prime. This is done to avoid potential subgroup leaks.

Ed25519 has a fast, efficient way to encode a point (x, y) into a 256-bit string.

Plan

Adding points

Two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ can be added with

$$P + Q = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 + x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$$

Wait, addition?

Addition?

Yes. There isn't much structure that is already defined with elliptic curves, so it is ok to pick any symbol we like. The symbol $+$ is handy.

This is, however, a source of confusion.

In $\mathbb{Z}_p^*$, we're used to	In elliptic curves, we have
$u \cdot v$	$P + Q$
1	0
u^{-1}	$-P$
exponentiation	scalar multiplication
square-and-multiply	double-and-add
$\mathrm{DLog}_{G,g}(h)$: k s.t. $g^k = h$	$\mathrm{DLog}_{E,P}(Q)$: k s.t. $Q = kP$

It's really the same set of concepts, but with a 1-to-1 dictionary translation.

Plan

Definition

The group law

In protocols

Diffie-Hellman

The curve Ed25519 is given.

A point P that generates the subgroup of prime order ℓ is given.

Alice choses x at random modulo ℓ, and sends $P_A = xP$.

Bob choses y at random modulo ℓ, and sends $P_B = yP$.

Alice computes xP_B and gets xyP.

Bob computes xP_A and gets xyP.

EdDSA signature scheme

EdDSA [BDLSY12] is a Schnorr-based signature scheme over an elliptic curve group.

Signing key sk is a random string of length a parameter b. It is expanded into a $2b$-bit string $x_1 \| x_2$. A clamping function is applied to x_1 to get the Schnorr signing key $x \in \mathbb{Z}_m$.

Signing is made deterministic by setting r to a hash of x_2 and the message.

There are several variants of the scheme.

These schemes are widely standardized, including RFC 8032 and FIPS 186-5. The scheme is used in many places including OpenSSH and GnuPG.

Other nice features of Ed25519

Parameters of Ed25519 are not "magic stuff with zero explanation".

Many possible implementation dangers are avoided by the several nice properties of the curve.

Computations are fast, and many implementations are available.

Security is good, since the DL problem is very hard. Nothing better than Baby-step Giant-step is known. Cryptanalysis costs 2^{128}.

CSE107: Intro to Modern Cryptography

https://cseweb.ucsd.edu/classes/sp22/cse107-a/

Emmanuel Thomé

June 2, 2022

Lecture 18c

A History of Cryptographic Backdoors

Export ciphers

Key escrow

Plan

Export ciphers

Key escrow

US export controls on cryptography

- Pre-1994: Encryption software requires individual export license as a munition.
- 1994: US State Department amends ITAR regulations to allow export of approved software to approved countries without individual licenses. 40-bit symmetric cryptography was understood to be approved.
- 1995: Netscape develops initial SSL protocol. Includes weakened "export" cipher suites.
- 1996: Bernstein v. United States; California judge rules ITAR regulations are unconstitutional because "code is speech"
- 1996: Cryptography regulation moved to Department of Commerce.
- 1999: TLS 1.0 standardized. Includes weakened "export" cipher suites.
- 2000: Department of Commerce loosens regulations on mass-market and open source software.

International Traffic in Arms Regulations

Category XIII--Auxiliary Military Equipment ...

(b) Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefore, including:

(1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software as follows:

(i) Restricted to decryption functions specifically designed to allow the execution of copy protected software, provided the decryption functions are not user-accessible.

(ii) Specially designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines, self-service statement printers, point of sale terminals or equipment for the encryption of interbanking transactions.

...

Commerce Control List, March 2021

2.a.A ‘‘symmetric algorithm’’ employing a key length in excess of 56 bits, not including parity bits;

2.b.An ‘‘asymmetric algorithm’’ where the security of the algorithm is based on any of the following:

2.b.1. Factorization of integers in excess of 512 bits (e.g., RSA);

2.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or

2.b.3. Discrete logarithms in a group other than mentioned in paragraph 2.b.2 of this Technical Note in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve); or

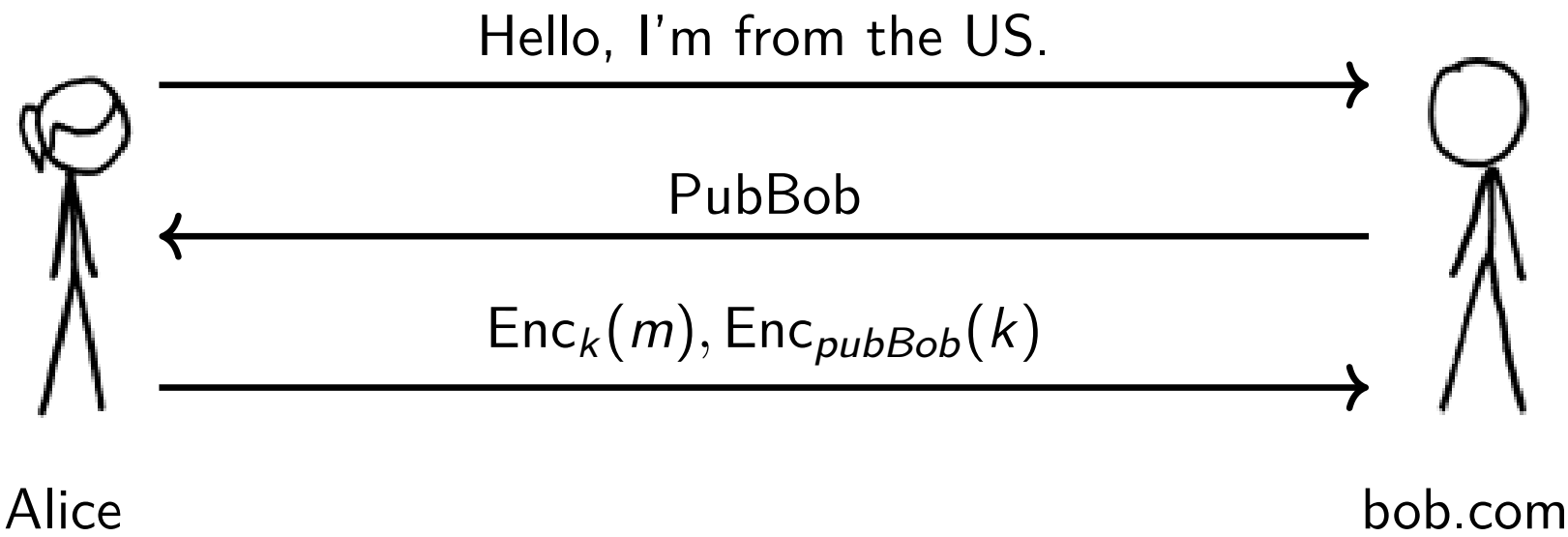
2.c. An ‘‘asymmetric algorithm’’ where the security of the algorithm is based on any of the following:

2.c.1. Shortest vector or closest vector problems associated with lattices (e.g., NewHope, Frodo, NTRUEncrypt, Kyber, Titanium);

2.c.2. Finding isogenies between Supersingular elliptic curves (e.g., Supersingular Isogeny Key Encapsulation); or

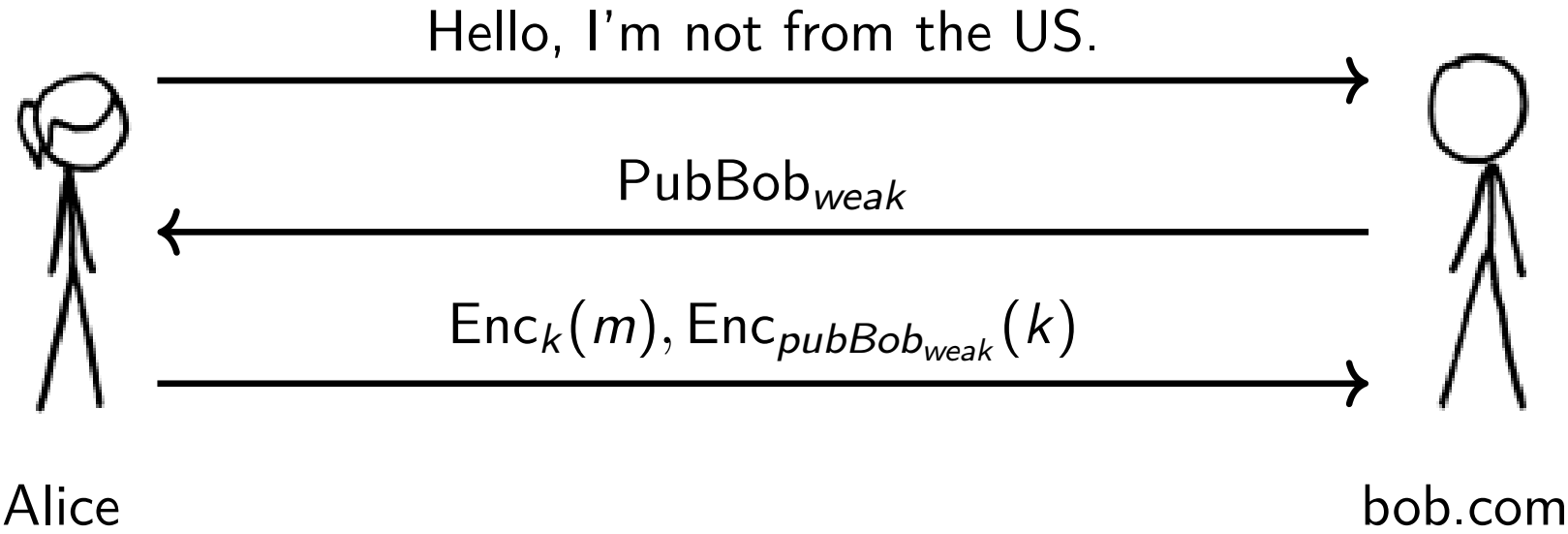
2.c.3. Decoding random codes (e.g., McEliece, Niederreiter).

"Export" cipher strength negotiation



PubBob is a strong public key and only Bob can decrypt the message.

"Export" cipher strength negotiation



- PubBob is weakened so that a large government could decrypt if significant resources invested.
- However, computation is not feasible for public, so web is safe for consumers.

Multi-decade fallout from US crypto export control

- Discouraged business in US
- Support for deliberately weakened "export-grade" cipher suites did not disappear in 2000, because vendors maintained backwards compatibility.
- 2015: FREAK, LogJam, and DROWN attacks exploited previously undiscovered SSL/TLS protocol flaws around negotiating export cipher suites. **10-25%** of popular web sites vulnerable.
- First public 512-bit factorization in 1999.
  - By 2015, 512-bit RSA could be factored by anyone for $75 in 3-4 hours on cloud computing.

Plan

Export ciphers

Key escrow

2G cipher weak

GEA-1 cipher designed in France in 1998 for use in 2G.

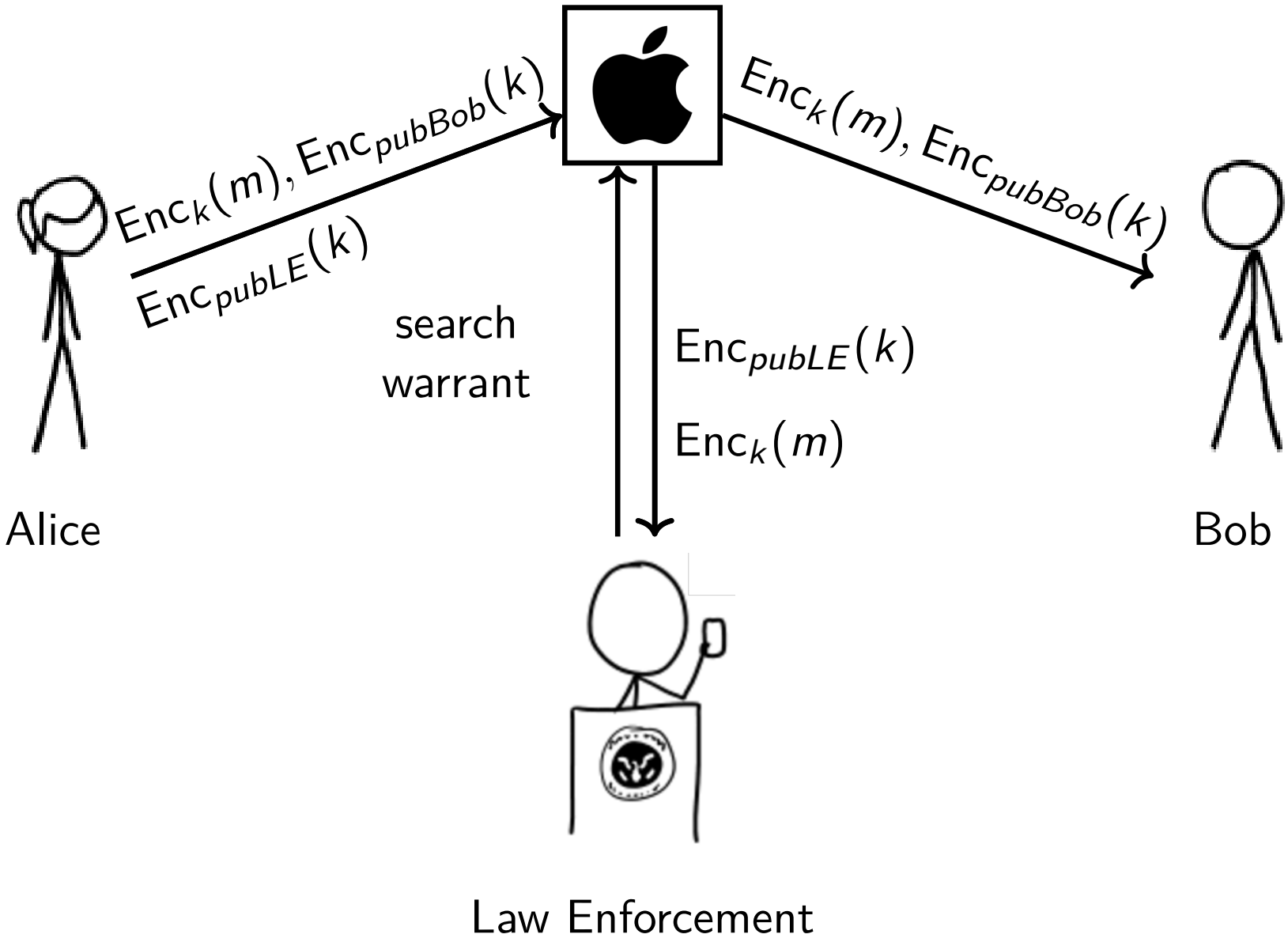
2021: Researchers discover 2^{40} attack.

"It was explicitly mentioned as a design requirement that 'the algorithm should be generally exportable taking into account current export restrictions' and that 'the strength should be optimized taking into account the above requirement'

Hypothesis: Algorithm designed to offer exactly 40 bits of security to comply with European export restrictions.

https://eprint.iacr.org/2021/819.pdf

A basic key escrow system



1993: NSA promotes "Clipper chip" key escrow

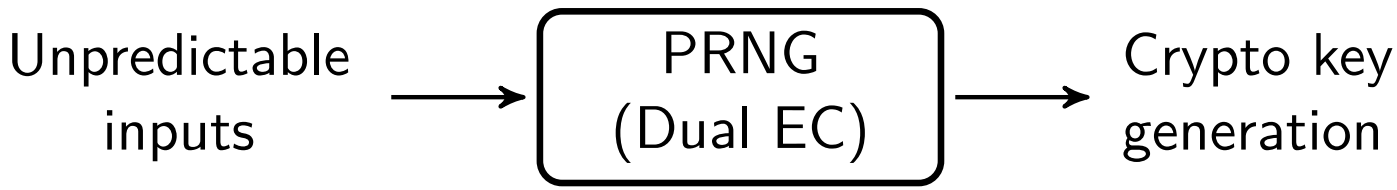
- Intended for voice transmission by telecommunications companies.
- Used Diffie-Hellman key exchange and Skipjack NSA-designed symmetric cipher with an 80-bit key.
- Secret keys were transmitted in a "Law Enforcement Access Field" to allow decryption with a warrant.
- 1994: Matt Blaze publishes protocol flaw allowing circumvention of key escrow.
- System abandoned by 1996.

Key escrow in theory and in practice

- In theory, key escrow is provably secure.
- In practice, schemes are difficult to secure.

Dual EC DRBG

- Pseudorandom number generator (PRNG) standardized by NIST, ISO.
- How to use a PRNG for cryptography:



- Dual EC design encodes backdoor/key escrow potential:
  - Algorithm designer can recover cryptographic secrets.
  - Cryptographically secure against all other parties.

Dual EC DRBG

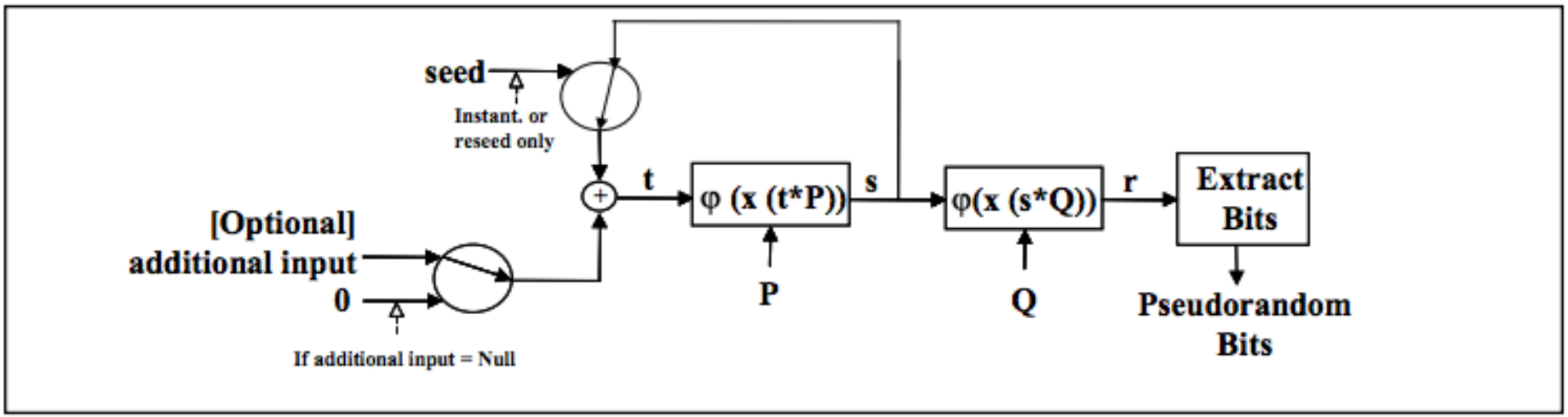


Figure 13: Dual_EC_DRBG

- Parameters: Pre-specified elliptic curve points P and Q.
- Seed: 32-byte integer s
- State: x-coordinate of point sP. ($\phi(x(sP))$ above.)
- Update: $t = s \oplus$ optional additional input. State $s = x(tP)$.
- Output: At state s, compute x-coordinate of point $x(sQ)$, discard top 2 bytes, output 30 bytes.

Timeline of Dual EC DRBG scandal

- Early 2000s: Created by the NSA and pushed towards standardization
- 2004: Published as part of ANSI X9.82 part 3 draft
- 2004: RSA makes Dual EC the default PRNG in BSAFE
- 2005: Standardized in NIST SP 800-90 draft
- 2007: Shumow and Ferguson demonstrate theoretical backdoor
- 2013: Snowden documents lead to renewed interest in Dual EC
- 2014: Practical attacks on TLS using Dual EC demonstrated
- 2015: NIST removes Dual EC from list of approved PRNGs

Still no way to prove standard was backdoored, or compromise traffic without knowing secret parameters.

How to exploit Dual EC backdoor

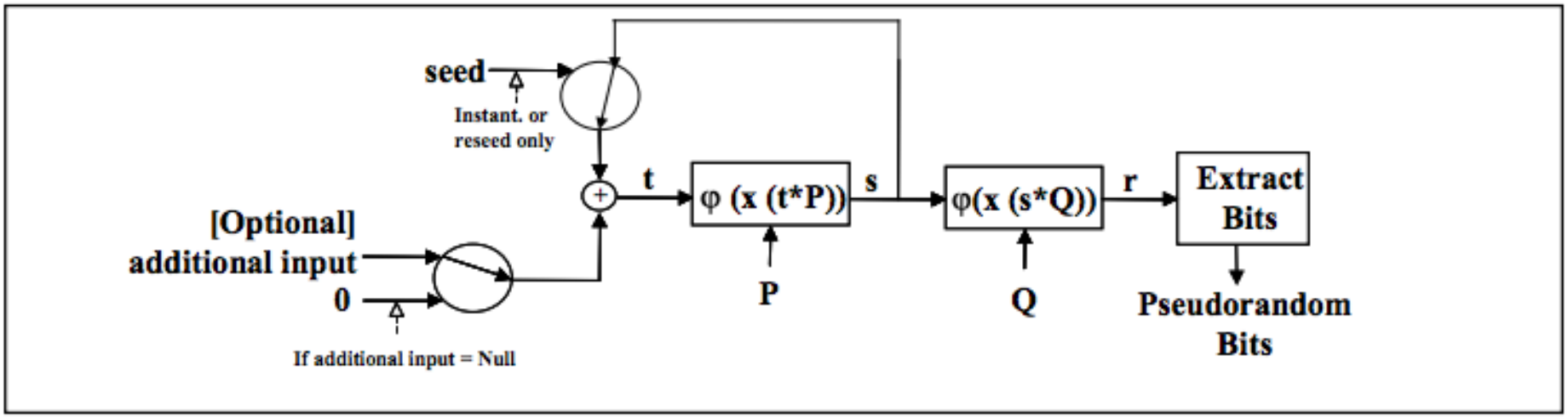


Figure 13: Dual_EC_DRBG

1. Assume attacker controls standard and constructs points with known relationship $P = dQ$.
2. Attacker gets 30 bytes of x-coordinate of sQ. Attacker brute forces 2^{16} MSBs, gets 2^{17} possible y-coordinates, ends up with 2^{15} candidates for sQ.
3. For each candidate sQ attacker computes $dsQ = sP$ and compares to next output.

September 2013: NSA Bullrun in NY Times

- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.
- (TS//SI//REL TO USA, FVEY) Collect target network data and metadata via cooperative network carriers and/or increased control over core networks.
- (TS//SI//REL TO USA, FVEY) Leverage commercial capabilities to remotely deliver or receive information to and from target endpoints.
- (TS//SI//REL TO USA, FVEY) Exploit foreign trusted computing platforms and technologies.
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- (TS//SI//REL TO USA, FVEY) Make specific and aggressive investments to facilitate the development of a robust exploitation capability against Next-Generation Wireless (NGW) communications.

Dual EC Attack Complexity in TLS Implementations

Table 1: Summary of our results for Dual EC using NIST P-256.

Library	Default PRNG	Cache Output	Ext. Random	Bytes per Session	Adin Entropy	Attack Complexity	Time (minutes)
BSAFE-C v1.1	✓	✓	✓†	31–60	—	$30 \cdot 2^{15}(C_v + C_f)$	0.04
BSAFE-Java v1.1	✓		✓†	28	—	$2^{31}(C_v + 5C_f)$	63.96
SChannel I‡				28	—	$2^{31}(C_v + 4C_f)$	62.97
SChannel II‡				30	—	$2^{33}(C_v + C_f) + 2^{17}(5C_f)$	182.64
OpenSSL-fixed I*				32	20	$2^{15}(C_v + 3C_f) + 2^{20}(2C_f)$	0.02
OpenSSL-fixed III**				32	$35 + k$	$2^{15}(C_v + 3C_f) + 2^{35+k}(2C_f)$	$2^k \cdot 83.32$

* Assuming process ID and counter known. ** Assuming 15 bits of entropy in process ID, maximum counter of 2^k. See Section 4.3.
† With a library–compile-time flag. ‡ Versions tested: Windows 7 64-bit Service Pack 1 and Windows Server 2010 R2.

the grugq
@thegrugq

Follow

Woah! Juniper discovers a backdoor to decrypt VPN traffic (and remote admin) has been inserted into their OS source

Important Announcement about ScreenOS®

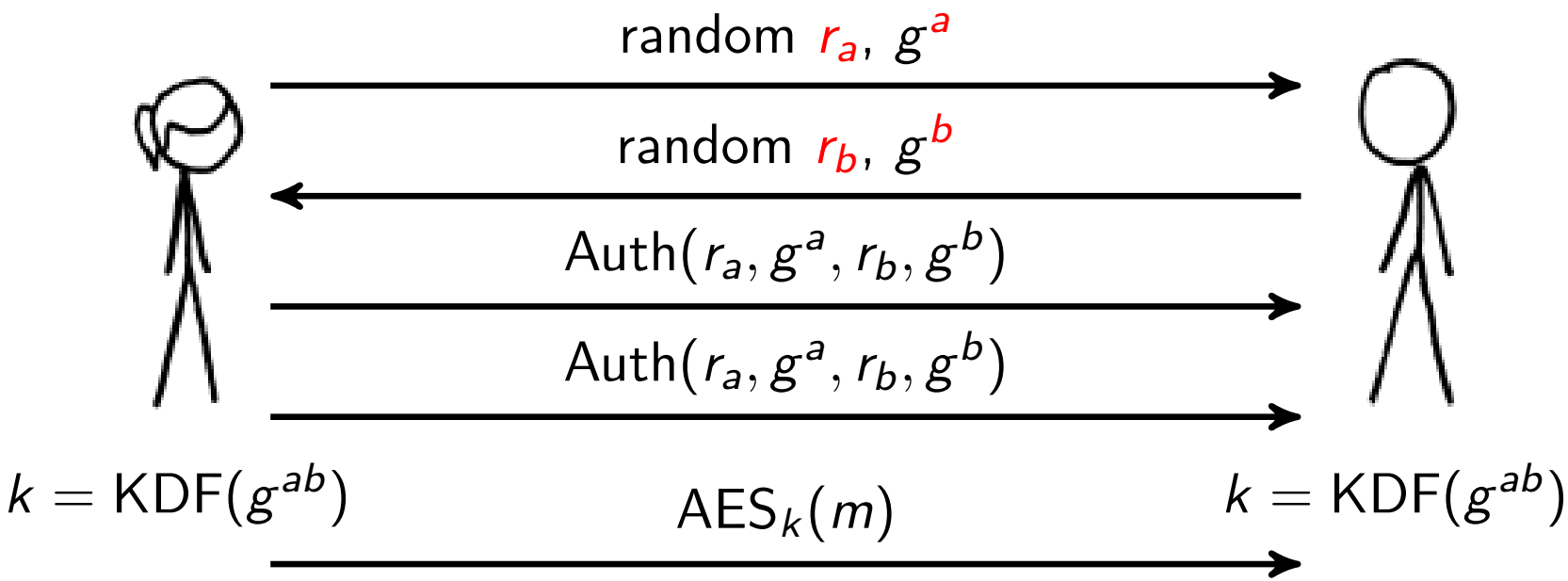
IMPORTANT JUNIPER SECURITY ANNOUNCEMENT CUSTOMER UPDATE: DECEMBER 20, 2015 Administrative Access (CVE-2015-7755) only affects ScreenOS 6.3.0r17 through

forums.juniper.net

Juniper ScreenOS Dual EC attack

- 2008: Juniper adopts Dual EC with countermeasures against theoretical backdoor.
- 2012: Unidentified attackers modified Juniper ScreenOS Dual EC implementation.
- 2015: Juniper discovers code modifications and publishes security advisory.
- 2016: Checkoway et al. observe that:
  1. Juniper's 2008 countermeasures contained a subtle bug: implementation enabled backdoor.
  2. Attacker had changed backdoor parameters.

Passive state recovery in ScreenOS IPsec



- Use random nonces to carry out state recovery attack.
- ScreenOS used 32-byte nonce $\Rightarrow$ efficient attack.
- After state recovered, then recover secret exponents.
- Researchers demonstrated attack with own backdoored P, Q.

ScreenOS Version History

ScreenOS 6.1.0r7

- ANSI X9.31
- Seeded by interrupts
- Reseed every 10k calls
- 20-byte IKE nonces

ScreenOS 6.2.0r0 (2008)

- Dual EC $\rightarrow$ ANSI X9.31
- Reseed bug exposes raw Dual EC
- Reseed every call
- Nonces generated before keys
- 32-byte IKE nonces

- Attacker changed constant in 6.2.0r15 (2012).
- But passive decryption enabled in earlier release.
- Juniper's "fix" was to reinstate original Q value. After academic analysis, they removed Dual EC completely.

September 2021: Publicly attributed to China

"Members of a hacking group linked to the Chinese government called APT 5 hijacked the NSA algorithm in 2012, according to two people involved with Juniper's investigation and an internal document detailing its findings that Bloomberg reviewed. The hackers altered the algorithm so they could decipher encrypted data flowing through the virtual private network connections created by NetScreen devices. They returned in 2014 and added a separate backdoor that allowed them to directly access NetScreen products, according to the people and the document."

https://www.bloomberg.com/news/features/2021-09-02/juniper-mystery-attacks-traced-to-pentagon-role-and-chinese-hackers

Lessons and discussion

- Attacker repurposed cryptographically secure key escrow/backdoor with small change to source code that went unnoticed for years.
- Juniper's *original implementation* contained critical vulnerabilities that went unnoticed for years.

Fallout: Simon and Speck controversy

NSA introduced two "lightweight" ciphers in 2013.

Submitted them to ISO for standardization.

Criticized for having too small of a security margin.

Mistrust of NSA led to rejection by ISO working group, though they were later adopted by other ISO working groups.

2019: suspicions over Russian ciphers

Russia standardized Streebog hash function and Kuznyechik block cipher, with GOST.

Submitted them to ISO: "if any abroad citizen, company or governmental structure have a wish to cooperate with Russian information services they have to implement these algorithms. We hope that international standardization will make this implementation easier."

Academics published articles finding several weaknesses.

Current Law Enforcement Access Debates

- 2016 Apple v. FBI
- Apple and Facebook CSAM detection algorithms.
- ...

Expectations for cryptographic design

How does an algorithm designer prove a lack of backdoors?

- Open analysis and standardization process.
- "Nothing up my sleeve" constants.
- Trust is a social process among humans.

Lessons and discussion

- Technical backdoors in our infrastructure don't go away when the political environment changes.
- Cannot assign cryptography based on nationality.
- Added complexity of special access introduces unexpected vulnerabilities.