6.857 Computer and Network Security
Lecture 16

Today:

- Digital signature standard
- “gap groups”
- Bilinear maps
- BLS digital signatures
- IBE (if time)

PEOPLE

Principal Investigators

All Members

Student Spotlights

Home » People » Daniel Weitzner

DANIEL WEITZNER

Position: Principal Research Scientist

Areas of Study: Privacy, Internet Policy, Web Architecture
Last Update: February 19, 2014

AWARDS
IAPP: Privacy Leadership Award (2013)
Newsweek/Daily Beast: Digital Power Index (2012)

submit new awards here: Award Registration Form

BIOGRAPHY

Daniel Weitzner is the Director of the MIT CSAIL Decentralized Information Group and teaches Internet public policy in MIT's Computer Science Department. His research includes development of accountable systems architectures to enable the Web to be more responsive to policy requirements.

From 20011-2012, Weitzner was the United States Deputy Chief Technology Officer for Internet Policy in the White House. He led initiatives on privacy, cybersecurity, Internet copyright, and trade policies promoting the free flow of information,. He was responsible for the Obama Administration's Consumer Privacy Bill of Rights and the OECD Internet Policymaking Principles.

Weitzner has been a leader in the development of Internet public policy from its inception, making fundamental contributions to the successful fight for strong online free expression protection in the United States Supreme Court, and for laws that control government surveillance of email and web browsing data.

Weitzner is a founder of the Center for Democracy and Technology, led the World Wide Wed Consortium's public policy activities, and was Deputy Policy Director of the Electronic Frontier Foundation. In 2012 he was named to the Newsweek/Daily Beast Digital Power Index as a top 'Navigator' of global Internet public policy and in 2013 he received the International Association of Privacy

Professional's Leadership Award.

<u>Digital Signature Standard</u> (DSS - NIST 1991)

<u>Public parameters</u> (same for everyone):

q prime $\qquad |q| = 160$ bits

$p = nq+1$ prime $\qquad |p| = 1024$ bits

g_0 generates Z_p^*

$g = g_0^n$ generates subgroup G_q of Z_p^* of order q

<u>Keygen:</u>

$x \xleftarrow{R} Z_q$ $\qquad$ SK $\qquad |x| = 160$ bits

$y \leftarrow g^x \pmod{p}$ $\qquad$ PK $\qquad |y| = 1024$ bits

<u>Sign (m):</u>

$k \xleftarrow{R} Z_q^*$ $\qquad$ (i.e. $1 \leq k < q$)

$r = (g^k \bmod p) \pmod{q}$ $\qquad |r| = 160$ bits

$m = h(M)$

$s = (m + rx)/k \pmod{q}$ $\qquad |s| = 160$ bits

<u>redo</u> if $r=0$ or $s=0$

$\sigma(M) = (r, s)$

Note: if k is reused for different messages m, one could solve for x so it is not secure. If k is reused for the same m, we obtain the same signature so this is not a problem. If k is different for the same m, it should be random and unknown (any known relation between the two k-s allows to solve for x)

Bottomline: All of the above are enforced by k chosen at random from Z_q^* for large enough q

Verify:

Check $0<r<q$ & $0<s<q$

Check $y^{r/s} g^{m/s} \pmod p)(\bmod q) = r$

where $m = h(M)$

Correctness:

$$g^{(rx+m)/s} \overset{?}{=} r \ (\bmod p)(\bmod q)$$

$$\equiv \quad g^{k} = r \ (\bmod p)(\bmod q) \qquad ✓$$

As it stands, existentially forgeable for h = identity.

Provably secure (as with Modified El Gamal)

if we replace $m = h(m)$ by $m = h(M \| r)$, as before.

Note: As with El Gamal, secrecy & uniquness of k

is essential to security.

TOPIC

DATE

FILE UNDER

PAGE L19.2

"Gap group" is one in which

- DDH is easy ("Decision Diffie Hellman")

  [Recall: given (g, g^a, g^b, g^c), to
  decide if $ab = c \pmod{\text{order}(g)}$
  ]

but

- CDH is hard ("Computational Diffie Hellman")

  [Recall: given (g, g^a, g^b), to
  compute g^{ab}

(Note that CDH easy $\Rightarrow$ DDH easy)

This difference in difficulty between DDH ("easy") and CDH ("hard") forms a "gap".

— How can one construct a "gap group"?

— What good would that be?