## 6.857 Computer and Network Security Lecture 16

Today:

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



SEARCH

ABOUT CSAIL

RESEARCH

Home » People » Daniel Weitzner

DANIEL WEITZNER

NEWS + EVENTS

RESOURCES

**ALUMNI & FRIENDS** 

PEOPLE

Principal Investigators All Members Student Spotlights



Position: Principal Research Scientist

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

**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 <u>Consumer Privacy Bill of Rights</u> and the <u>OECD Internet Policymaking Principles</u>.

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.

Massachusetts Institute of Technology

## AWARDS

PEOPLE

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

submit new awards here: <u>Award</u> <u>Registration Form</u>

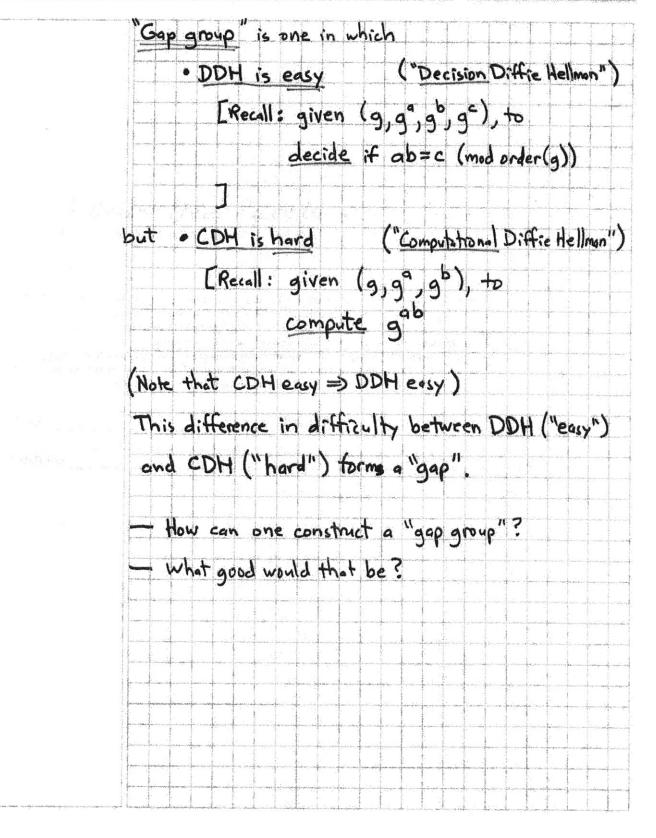
f 🕒 🐨 👯

$$E_{2,2} = E_{2,2} = E_{2$$

**KOPIC** OF DWARE PASI L17.10 Verify : Check Orrig & orsky Check y g m/s (mod p) (mod g) = r where m=h(M) Correctness: g(rx+m)/s ? r'(mod p)(mod g) gh = r (mod p) (mod g) -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 Gamel, secrecy & uniqueness of k is essential to security.

4

PAGE 119 5
L1, a



```
ÎÈİİÞ^ç [¦\Áse) åÁÔ[{]čo\¦ÁÙ^&č¦ãĉ
Spring 2014
```

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.