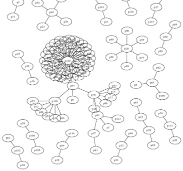
Presentation at Department Dialog

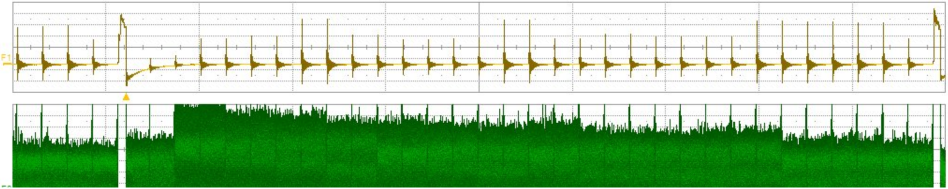
Tanja Lange

November 21, 2013

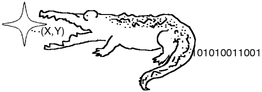
I like breaking things



- Factored nearly two hundred RSA-1024 keys on TW citizen cards (certified smart cards) smartfacts.cr.yp.to.
- Decoded a message in original McEliece cryptosystem.
- Big discrete log computation (ongoing) ecc-challenge.info.
- Side-channel analysis of ARM processors.

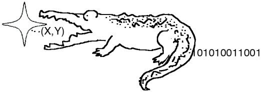


I like making things



- Secure cryptographic signatures `ed25519.cr.yp.to`.
- Indistinguishable maps to elliptic curves `elligator.cr.yp.to`.
- Intrinsic keys from standard hardware `puffin.eu.org`.
- Cryptographic library NaCl `nacl.cr.yp.to` and better protocols for the Internet (MinimaLT).
- Explicit Formulas Database `hyperelliptic.org/EFD` for elliptic curves.

I like making things



- Secure cryptographic signatures ed25519.cr.yp.to.
- Indistinguishable maps to elliptic curves elligator.cr.yp.to.
- Intrinsic keys from standard hardware puffin.eu.org.
- Cryptographic library NaCl nacl.cr.yp.to and better protocols for the Internet (MinimaLT).
- Explicit Formulas Database hyperelliptic.org/EFD for elliptic curves.
- Due to certain mistrust in NIST/NSA safecurves.cr.yp.to with new, better elliptic curves.

Use crypto!

- Despite mistrust in NIST etc.: Some crypto is better than none.
- Guilt by association: Three hops away from target are surveilled when target is tasked.

Use crypto!

- Despite mistrust in NIST etc.: Some crypto is better than none.
- Guilt by association: <u>Three</u> hops away from target are surveilled when target is tasked. I might be a target (researcher in crypto)

Use crypto!

- Despite mistrust in NIST etc.: Some crypto is better than none.
- Guilt by association: Three hops away from target are surveilled when target is tasked. I might be a target (researcher in crypto) or one hop away from a target,

Use crypto!

- Despite mistrust in NIST etc.: Some crypto is better than none.
- Guilt by association: Three hops away from target are surveilled when target is tasked. I might be a target (researcher in crypto) or one hop away from a target, which brings all of you in the range of interest.

Use crypto!

- Despite mistrust in NIST etc.: Some crypto is better than none.
- Guilt by association: Three hops away from target are surveilled when target is tasked. I might be a target (researcher in crypto) or one hop away from a target, which brings all of you in the range of interest.
- Sign important messages: marks from exams, promises of funding, . . .
- Encrypt confidential data: exams, data from consulting contracts

Use crypto!

- Despite mistrust in NIST etc.: Some crypto is better than none.
- Guilt by association: Three hops away from target are surveilled when target is tasked. I might be a target (researcher in crypto) or one hop away from a target, which brings all of you in the range of interest.
- Sign important messages: marks from exams, promises of funding, . . .
- Encrypt confidential data: exams, data from consulting contracts
- Keep your privacy!

Easy: Use PGP/GPG

- Download GPG4win for windows, GPGtools for MAC-OS, or GPG for linux.
- Generate keys – you'll have a secret key and a public key. Under windows this is done with the GPA program.
- Save secret key in a secure place (USB stick that stays in your pocket, encrypted disk with Truecrypt, ...)
- Send public key to your friends & colleagues, put it on your website, put it on keyservers. Under windows this is done with the Kleopatra tool.
- Encrypt files or text in clipboard with GPA tool. Use Claws Mail (part of the package), or Enigmail (with Thunderbird), or a plugin for Windows Outlook.

Easy: Use PGP/GPG

- Download GPG4win for windows, GPGtools for MAC-OS, or GPG for linux.
- Generate keys – you'll have a secret key and a public key. Under windows this is done with the GPA program.
- Save secret key in a secure place (USB stick that stays in your pocket, encrypted disk with Truecrypt, ...)
- Send public key to your friends & colleagues, put it on your website, put it on keyservers. Under windows this is done with the Kleopatra tool.
- Encrypt files or text in clipboard with GPA tool. Use Claws Mail (part of the package), or Enigmail (with Thunderbird), or a plugin for Windows Outlook.
- Just try it (and maybe read the manual – or send me encrypted messages as a test).

Check out more programs that are good for your privacy on `https://prism-break.org/`.