

Introduction to Computer Security Lecture Slides

© 2024 by [Mihai Chiroiu](#) & [Florin Stancu](#)

is licensed under [Attribution-NonCommercial-ShareAlike 4.0
International](#)

Privacy Preserving Technologies

Objectives

- Internet Tracking
- Regulation: GDPR, IAPP
- Privacy solutions:
 - VPNs
 - Mix Nets / Onion routing / TOR
 - Private Information Retrieval (PIR)
 - ORAM
- Decentralization

Motivation

“There was of course no way of knowing whether you were being watched at any given moment...You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard and, except in darkness, every movement scrutinized.”

– George Orwell, 1984 (1948)

Digital Privacy

- “There is no privacy in the digital age.”
 - Ubiquitous data collection
 - Mobile platform duopoly
- “No one cares about privacy anymore.”
 - Centralized social networks
- “If you haven’t done anything wrong you have nothing to hide.”
 - *yet...*
- Stolen address databases fuels global SPAM mails!

How are we tracked?

- Source IP address, traffic sniffing (e.g., DNS requests)
- Behavioral Tracking
- Browser / device fingerprinting
- Web tracking:
 - Cookies
 - Pixels
 - Ads
 - Third party JavaScript (e.g., social network snippets / marketing / analytics)
- Centralization (CDNs / social media / browser monopoly etc.)

Mass Surveillance / Legal Tracking

- UKUSA (1941)
 - The Five Eyes: USA, Australia, Canada, New Zealand, and the UK
 - In 1975 the United States revealed the existence of the NSA
- ECHELON (1971)
 - mass surveillance and industrial espionage
- Communications Assistance for Law Enforcement Act (CALEA, 94)
 - “China had been tapping communications in the U.S. using that infrastructure for months” 😓
- PRISM (2007):
 - collects network traffic from all US major online service providers
 - must have warrant to intercept traffic
- TEMPEST: spying through leaking EM emanations

Legitimate reasons

Hacker-ul roman care a spart serverele NASA a fost retinut de procurorii DIICOT

Un hacker roman, care i-a pus pe jar pe informaticienii de la NASA, a fost retinut astazi la Cluj. Procurorii americani au cerut sprijinul autoritatilor romane pentru a-l retine pe tanarul de 26 de ani.

U.S. Charges Russian Man as Boss of LockBit Ransomware Group

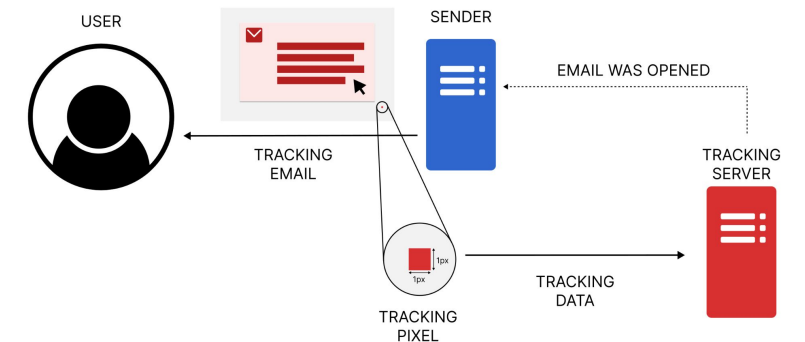
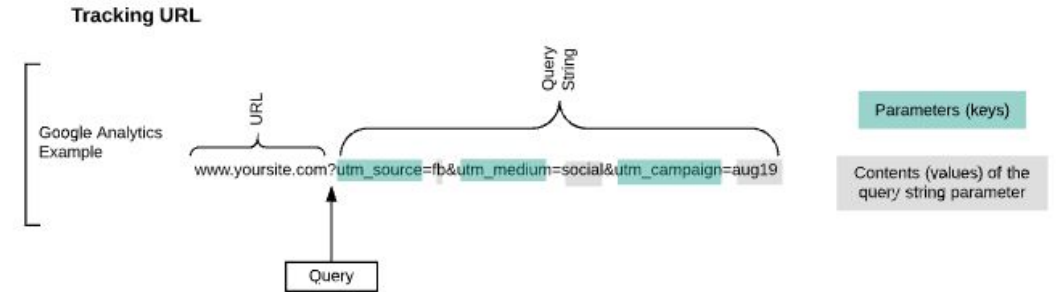
May 7, 2024

1 Comment

The United States joined the United Kingdom and Australia today in sanctioning 31-year-old Russian national **Dmitry Yuryevich Khoroshev** as the alleged leader of the infamous ransomware group **LockBit**. The **U.S. Department of Justice** also indicted Khoroshev and charged him with using Lockbit to attack more than 2,000 victims and extort at least \$100 million in ransomware payments.

Web Tracking

- HTTP Origin request header
- Tracking URLs
 - via query string parameters
- Cross-Site Tracking Cookies/JavaScript
 - Google Analytics, Facebook/Twitter/TikTok Share widgets etc.
- Spy Pixel
 - Email client makes remote request to display image, contains unique ID / email hash



Device Fingerprinting

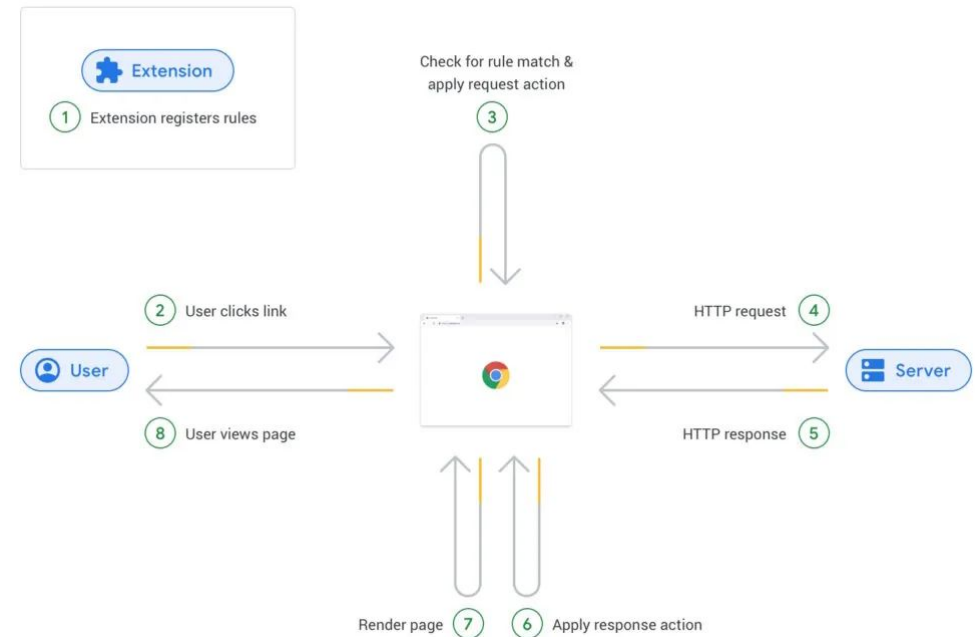
- Build a multi-variable vector:
 - User's IP address + Geo Location, VPN / local network IP address
 - Operating System / User agent / browser version
 - HTTP request headers
 - Cookies / history (:visited colors on links – by JS)
 - Plugins / fonts / browser extensions
 - Screen resolution / battery info / CPU/GPU statistics
 - Settings (time zone, language)
- Identify user across networks & devices => Profit!

Cloud centralization

- Cloud hosting & CDNs:
 - CloudFlare, Google, AWS
 - TLS connections are terminated by cloud provider ingress servers!
- Hosted libraries / fonts
 - Load JS libraries from Google & GitHub
 - Web-based font requests logged
- Behavioral tracking: websites + social media
 - Marketing dept. dream: mouse pointer tracking -> Heat Map
 - Doom Scrolling -> user pauses -> record interests!

Web Browser Monopolies

- IE 5-8 era: Microsoft controlled “*web standards*”
- 2024: Google controls web standards..
- Google Chrome: Manifest v3
 - Removed *webRequest* API
 - Use declarative Net Req. API instead!
 - Rules limit, no behavioral ad blocking...
 - No uBlock for you!
- Federated Learning of Cohorts (FLoC)



Corporate Harvesting

- Commercial: Amazon, Google, Facebook, Apple [12]
- Data Brokers (information resellers):
 - Target services: marketing / advertising, financial services / fraud detection, people search etc.;
 - Data acquisition: web tracking, public record scraping, commercial sharing/selling (by card transactions, retailers & advertising companies)
- How? You simply agree to it (check License Agreement)
- Government agencies often bypass warrant requirements by doing commercial agreements with companies (:

Regulatory approach: GDPR

- “The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world.”
- Disclose any data collection
- Right to be forgotten
- Data minimisation
 - Only collect / store required personal information
- Exemptions: law & national security
- Downloading / exporting your personal data from providers

I'm glad Swedish television is taking seagull privacy so seriously



GDPR effects

TECH

French watchdog slaps Google with \$57 million fine under new EU law

PUBLISHED MON, JAN 21 2019 11:58 AM EST | UPDATED MON, JAN 21 2019 12:29 PM EST

AP

SHARE [f](#) [t](#) [in](#) [✉](#)

The GDPR is no longer the only data protection acronym to pay attention to

The GDPR has inspired many imitators, from [Brazil's LGPD](#) to the [CCPA in California](#). While many of these laws agree on the broad terms of data protection, each implements these protections in its own way. And these two new regulations are just the start: [Canada](#) and Australia are both considering new data protection regulations, and India's legislature will vote on its [Personal Data Protection Bill](#). In the US, [several states](#), including Nevada, New York, Texas, and Washington, are considering following California's lead and passing their own data protection law.

YOUR LOGO

Powered by **Cookiebot**
by Usercentrics

Consent

Details

About

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary

☐

Preferences

☐

Statistics

☐

Marketing

☐

Deny

Allow Selection

Allow all

IAPP

- GDPR training?
- International Association of Privacy Professionals
 - <https://iapp.org/certify/programs/>



Definitions

- *Anonymity*: The state of being unidentifiable
- *Pseudonymity* is the use of pseudonyms as IDs and allows to provide both privacy protection and accountability
- *Unobservability* ensures that a user may use a resource or service without others being able to observe that the resource or service is being used
- *Unlinkability* of sender and recipient (relationship anonymity) means that it is untraceable who is communicating with whom

Privacy-Enhancing Technologies

- 1. PETs for minimizing/avoiding personal data (Anonymity, Pseudonymity, Unobservability, Unlinkability)
 - At communication level (VPN, MixNet, Onion Routing, TOR, Crowds)
 - At application level (Anonymous Ecash, Private Information Retrieval, Anonymous Credentials)
- 2. PETs for the safeguarding of lawful processing
 - Platform for Privacy Preferences Project (P3P) / Do Not Track
 - Privacy policy languages
 - Transparency Enhancing Tools (TETs)
- Combination of 1 & 2
 - Privacy-enhanced Identity Management

VPNs

- **Virtual Private Network**
- Use cases: business (corporate) / user privacy (consumer)
- Consumer VPN services
 - for privacy / bypass geoblocking (e.g., Netflix) & censorship
 - E.g.: ProtonVPN, ExpressVPN, NordVPN, Mullvad etc.
- Anonymization & logging
- Security Vulnerabilities
 - **Hot!** *Tunnel Vision* (CVE-2024-3661) [13]

CVE-2024-3661

- Static route injection via DHCP option 121 will bypass any VPN default GW :D
- Most VPN services & OS platforms are vulnerable

Typical routing table when using VPN:

```
141.85.241.131/32 via 192.168.0.1 dev eth0 metric 100
10.13.37.0/30 dev tun0 scope link src 10.13.37.2 metric 100
192.168.0.0/24 dev eth0 scope link src 192.168.0.100 metric 100
0.0.0.0/0 via 10.13.37.1 dev tun0 metric 50
```

CVE-2024-3661

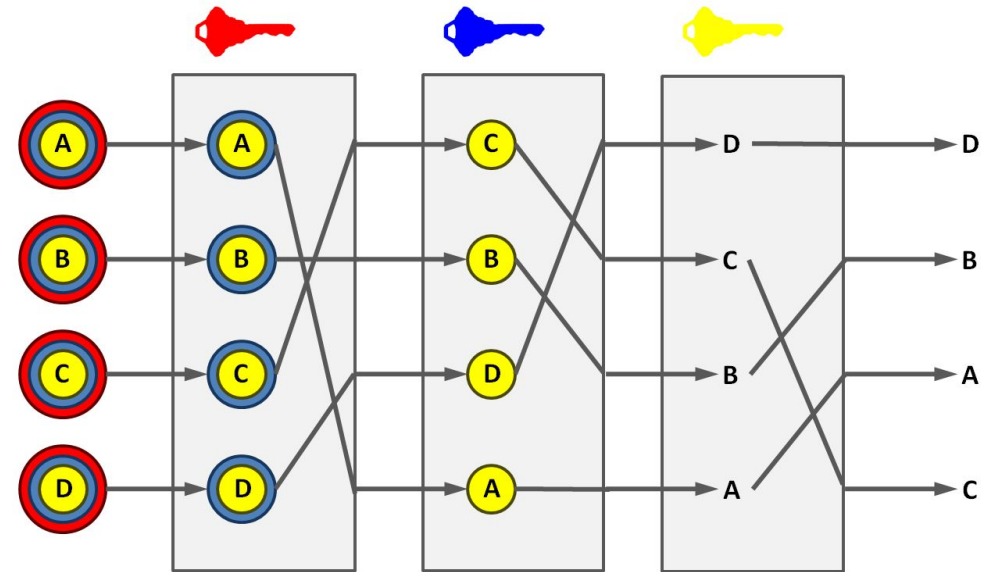
- Static route injection via DHCP option 121 will bypass any VPN default GW :D
- Most VPN services & OS platforms are vulnerable

Typical routing table after DHCP option 121 static route attack:

```
141.85.241.131/32 via 192.168.0.1 dev eth0 metric 100
10.13.37.0/30 dev tun0 scope link src 10.13.37.2 metric 100
192.168.0.0/24 dev eth0 scope link src 192.168.0.100 metric 100
0.0.0.0/1 via 192.168.0.1/24 dev eth0 metric 100
0.0.0.0/0 via 10.13.37.1 dev tun0 metric 50
```

Mix Networks

- Use one or many proxy servers, mixing traffic
- Input encrypted with public key of mixer
- Mixer decrypts and extracts next hop address
- Anonymization of sender – destination relationship
- High Latency: mixer must wait & aggregate multiple messages before sending them

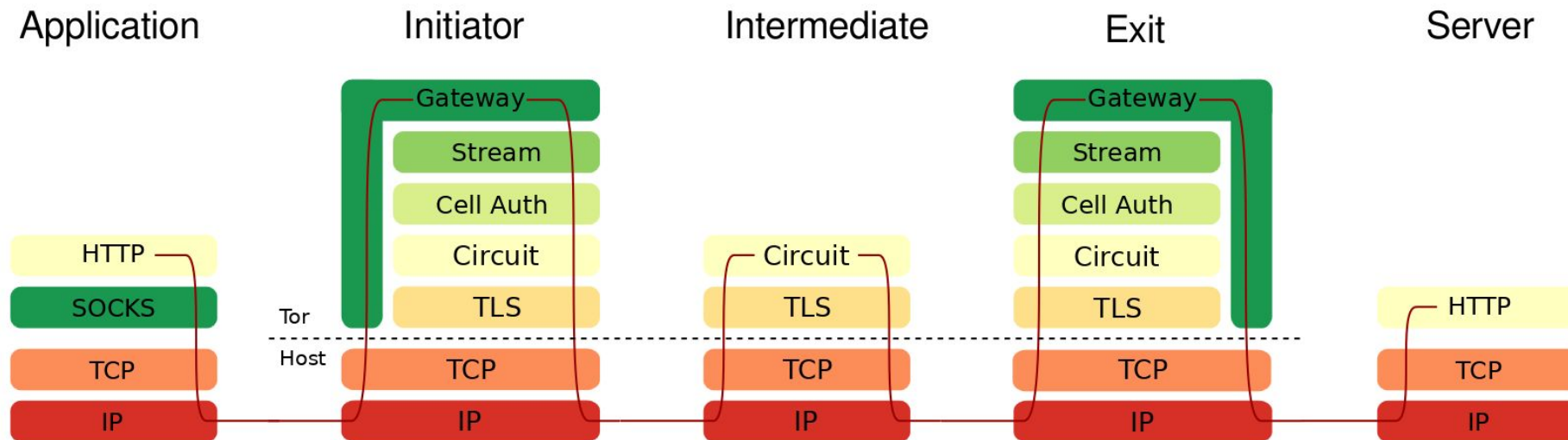


Onion routing

- Originator pick path through multiple nodes, encrypts packet in multiple layers with each node's public key (Matryoshka-like encapsulation)
- Each intermediary node decrypts with own key and forwards it
- Result: anonymization overlay network
- First + Last-Hop-based vulnerabilities in low-latency networks:
 - Timing correlations
 - Message length (No. of packets traversing network)

TOR

- No mixing is employed, just onion network overlay (low-latency)
- Uses SOCKS encapsulation of application traffic
- TOR server may be hosted on separate device (e.g., Raspberry PI)

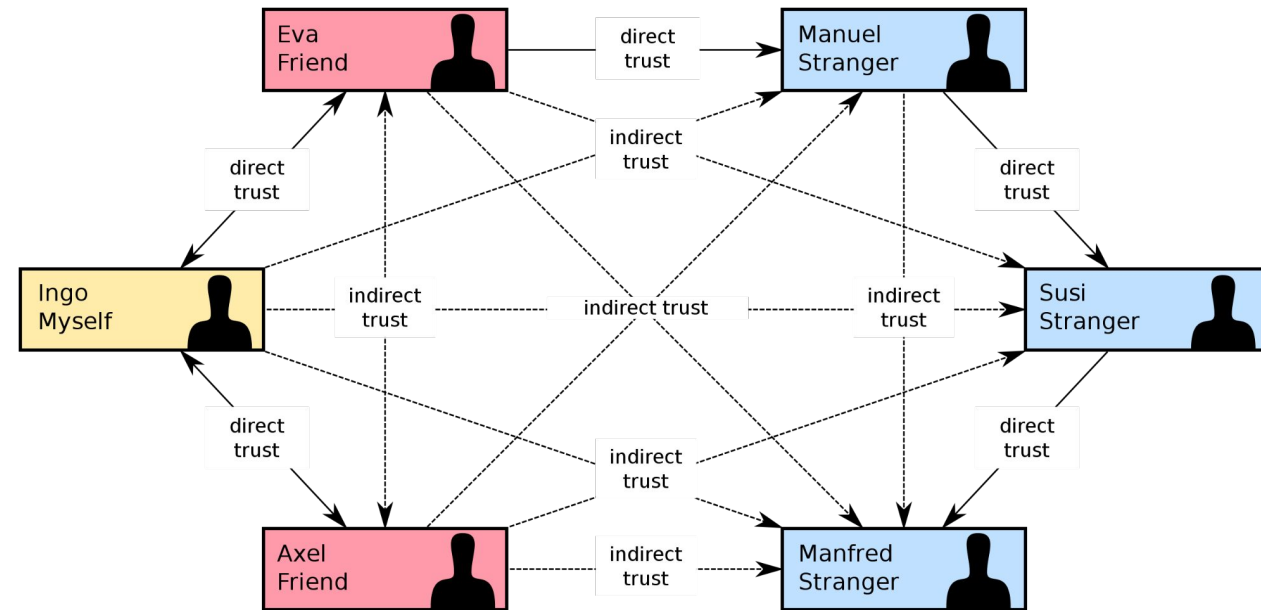


Mixnets vs Onion Routing

- “Tor plays with space alone (the bytes that you send across the network go through various other servers thus they aren’t where they are supposed to be) and mixnets play with both space and time (adds delays and shuffles the request through various servers as well).”

Pretty Good Privacy

- Web-of-Trust
 - Peer-to-peer model
 - Individuals digitally sign each other keys
 - Different levels of trustworthiness
 - E.g.: ultimately trust your friends
- Implementation: **gpg**
 - Used by Linux package managers, git signatures, pass manager etc.
- Unpopular due to UX/learning curve
- <https://keys.openpgp.org/>



Off the record protocol [11]

- Problem: peer to peer chat, end to end encryption
- Use PGP? Long term private key compromised => entire chat history becomes decryptable!
- OTR => perfect forward secrecy!
- Non-repudiability vs **forgeability**
 - Use Malleable Encryption:
 - change 1 bit in plain text => changes in ciphertext, too!
 - XOR-based cipher, e.g.: stream / CTR / GCM block modes etc.

Private Information Retrieval (PIR)

- Privacy for the item of interest:
 - Allows a user to retrieve an item from a database server without revealing which item he is interested in
- Application example: patient database
- Simple (but expensive) solution:
 - Download all database entries and make local selection
- Cryptographic generalization: Oblivious Transfer (OT [14])

Oblivious RAM

- Problem: Trusted Execution Environments, encrypted RAM...
 - have location + timing side channels => data is still insecure!
- Oblivious RAM: compiler that translates code to another one, same function, randomized memory access patterns
- Naive implementation: for each read/write instruction, do a full memory scan => $O(n)$ overhead!
- More efficient (but simple) methods exist: Path ORAM [15]

Web Privacy

- Don't use big tech-owned browsers (Chrome, Edge)
- Use Open Source variants: Firefox ~~& Chromium~~
- Privacy extensions:
 - Privacy Badger
 - uBlock Origin / Adblock
 - Disconnect
 - Ghostery, LocalCDN, DecentralEyes etc.
- Block / isolate third party cookies (e.g.: Facebook Container)
- Use Encrypted DNS (**dnscrypt-proxy** / Firefox DNS over HTTPS)!

Privacy: future work

- Decentralized social networks (Mastodon, Bluesky)
- Personal Cloud (e.g., Self-Hosted on a Raspberry PI)
 - pi-hole: local network ad-blocking / privacy proxy & DNS
- Use privacy-focused OSes / apps
 - Tails: Amnesia Incognito Live System
 - Sandboxed Applications (Containers)

Decentralized Currencies

- E.g.: Bitcoin, Ethereum, Monero, DogeCoin etc.
- Blockchain: huge transaction ledger cryptographically protected from modification
- Consensus: Proof of Work vs Proof of Stake
- Anonymization via mixers (alt name: tumblers)!
- Issues: no rollback, energy-intensive, financial fraud, money laundering etc.

References

[1]

<https://csjourney.com/onion-routers-mix-networks-differences-explained/?fbclid=IwAR3DPEKLM1-Zee--9VbpWfdTH0qn-RRMG5e8K2CTjrPCBzBYgJI5PsTC6FQ>

[2] <https://gdpr.eu/>

[3] <https://iapp.org/>

[4]

<https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf>

[5] <https://www.cs.kau.se/cs/education/courses/dvad03/p2/>

References

- [6] https://en.wikipedia.org/wiki/UKUSA_Agreement
- [7] [https://en.wikipedia.org/wiki/Tempest_\(codename\)](https://en.wikipedia.org/wiki/Tempest_(codename))
- [8] <https://petsymposium.org/2011/papers/hotpets11-final10Syverson.pdf>
- [9] https://link.springer.com/content/pdf/10.1007/3-540-47721-7_31.pdf
- [10] <https://www.activism.net/cypherpunk/manifesto.html>

References

- [11] <https://otr.cypherpunks.ca/otr-wpes.pdf>
- [12] <https://www.security.org/resources/data-tech-companies-have/>
- [13] <https://www.leviathansecurity.com/blog/tunnelvision>
- [14] <https://www.youtube.com/watch?v=wE5cl8J27Is>
- [15] <https://eprint.iacr.org/2013/280.pdf>