西安交通大學
XI'AN JIAOTONG UNIVERSITY

第 1 章：密码学简介

1.2 应用举例

赵俊舟

junzhou.zhao@xjtu.edu.cn

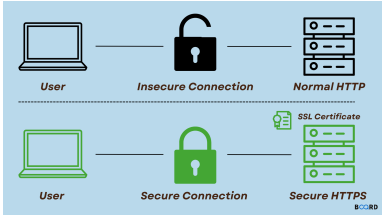
2025 年 2 月 20 日

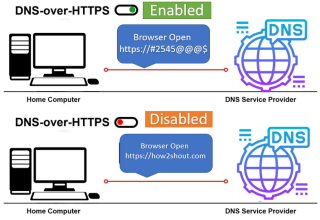
目录

目录

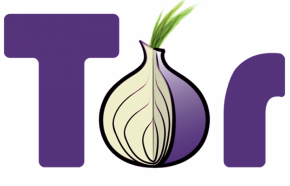
应用 1：加密通信

- 加密通信协议：HTTPS, DNS over HTTPS 等

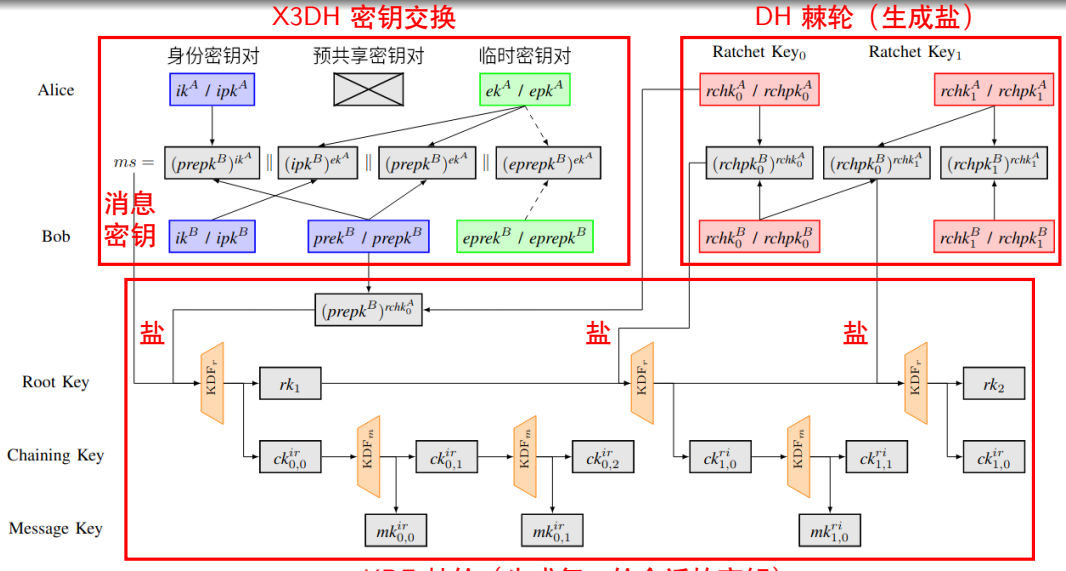




- 加密消息：Signal, WhatsApp
- 匿名网络：Tor, Yandex



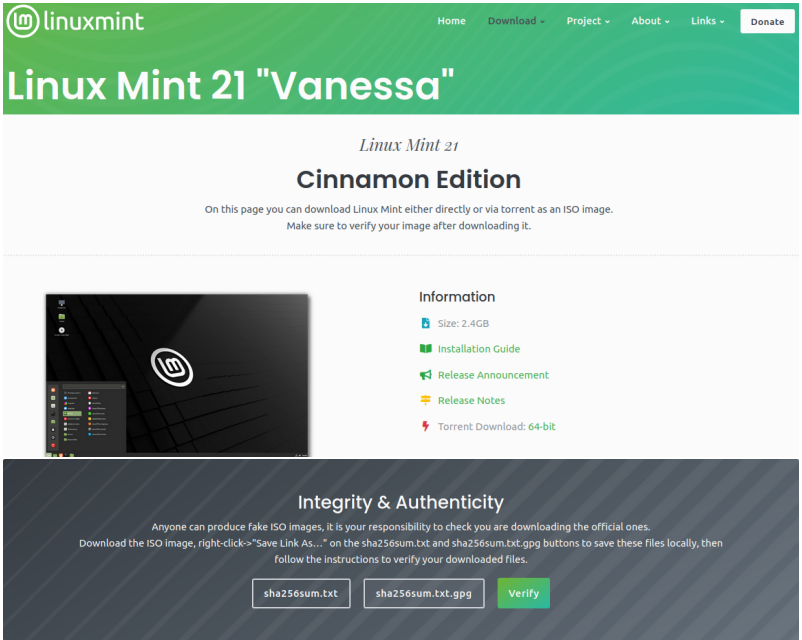
应用 1：Signal 端到端加密核心协议



Katriel et al. A formal security analysis of the signal messaging protocol. EuroS&P, 2019.

目录

应用 2：消息认证与数字签名



应用 2：消息认证与数字签名

Linux Mint website hacked, ISO downloads replaced with backdoored operating system

If you downloaded Linux Mint on Saturday, February 20th, you may have grabbed a hacked version that includes a backdoor. Here's what you need to know.

By Nick Mediati
PCWorld | FEB 21, 2016 10:02 AM PST

If you downloaded Linux Mint on Saturday, February 20th, you may have unknowingly downloaded a hacked version of the operating system.

According to a blog post on the Linux Mint site, hackers broke into the Linux Mint website at some point on Saturday and made changes in order to direct users toward downloading "a modified Linux Mint ISO, with a backdoor in it." Using the hacked version could allow hackers to steal your private information. According to Linux Mint, the hack only affects those who downloaded the Linux Mint 17.3 Cinnamon edition from the Linux Mint website on Saturday.

应用 2：消息认证与数字签名

文件内容：三个 ISO 文件的消息摘要及消息摘要的数字签名。

```
→  linuxmint ls -l
total 2839692
-rw-rw-r-- 1 jzzhao jzzhao 2907832320 Nov  6 20:04 linuxmint-22-cinnamon-64bit.iso
-rw-rw-r-- 1 jzzhao jzzhao        286 Nov  6 20:15 sha256sum.txt
-rw-rw-r-- 1 jzzhao jzzhao        833 Nov  6 20:09 sha256sum.txt.gpg
→  linuxmint cat sha256sum.txt
7a04b54830004e945c1eda6ed6ec8c57ff4b249de4b331bd021a849694f29b8f *linuxmint-22-cinnamon-64bit.iso
78a2438346cfe69a1779b0ac3fc05499f8dc7202959d597dd724a07475bc6930 *linuxmint-22-mate-64bit.iso
55e917b99206187564029476f421b98f5a8a0b6e54c49ff6a4cb39dcfeb4bd80 *linuxmint-22-xfce-64bit.iso
→  linuxmint cat sha256sum.txt.gpg
-----BEGIN PGP SIGNATURE-----

iQIzBAABCgAdFiEEJ96xVkTGs88719KRMA+Ea6JbrgkFAmaenwYACgkQMA+Ea6Jb
rgmbVRAAnrlVmEBRWce/lwImwzjEj3FIDwJ7OA4h9+gnBVJmXysjY0/ubZTBkFGE
M/5wOgQfyAO6m89zRhcyCo6nG4MHXdJ15AenuTBER5V/i4cN/VCN0x0ktCyKQG7o
pXLiVKp5LqY2acdiwjaJQIYBuLDuaTuMJSFgYA/dhuTy6u2U3Av1due2Q0rass5y
8Wkn0OsnS4yQiRLQYgHji1Kg7CBG5GyycZFLt+vYVDbw4U5vVQ8Dxv1gDxnNbT6j
uNySskMicQuqVkadiF2jykWTTILfBfsl7l44AZBsJdrT9jQrcaNFiRjea00x0FF9
+CZDFdcriKcAhyw+dVLeJeUFzmFha7o0czSop2KOLQHCC866ikYX9SvCy5kYD4et
O+bNOXA/W/PaVtjhRxIMgZfWYJjZD4EYNyAWunyYbT/mq2WFlKWc34V3mu1343my
AbxmdzaWIfPpADIMqf2cJrm3FaDictUfvyQ21g9GZR2nKV9U+OYEy7+LQZlLf3Vn
e0KnsO+LD5DBOjiRd12mgGZX05abIhoH7SYFppuIyWxe1Sc2Yp8h1RMhE6uo4PBA
fRThx4T3v5q+GmN7lmtvCpxkuVFr0FxHUpHuMDxNRo2IwJOTyJQu+Ult6oRoEaHY
iX2NkgmIt5LQ+UdyT0ol6KqsfxlU/0yrkJjctC6Nu8hJdwrCAmQ=
=hr4l
-----END PGP SIGNATURE-----
```

应用 2：消息认证与数字签名

文件完整性验证：确定所下载的文件是否被篡改过

```
→  linuxmint sha256sum -c sha256sum.txt
linuxmint-22-cinnamon-64bit.iso: OK
sha256sum: linuxmint-22-mate-64bit.iso: No such file or directory
linuxmint-22-mate-64bit.iso: FAILED open or read
sha256sum: linuxmint-22-xfce-64bit.iso: No such file or directory
linuxmint-22-xfce-64bit.iso: FAILED open or read
sha256sum: WARNING: 2 listed files could not be read
```

身份验证：确定所下载的文件是否来自官方

```
→  linuxmint gpg --verify sha256sum.txt.gpg sha256sum.txt
gpg: Signature made Tue 23 Jul 2024 02:03:50 AM CST
gpg:                using RSA key 27DEB15644C6B3CF3BD7D291300F846BA25BAE09
gpg: Good signature from "Linux Mint ISO Signing Key <root@linuxmint.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 27DE B156 44C6 B3CF 3BD7  D291 300F 846B A25B AE09
```

应用 2：消息认证与数字签名

篡改消息摘要：等效于篡改 ISO 文件内容

```
→  linuxmint vi sha256sum.txt
→  linuxmint cat sha256sum.txt
8a04b54830004e945c1eda6ed6ec8c57ff4b249de4b331bd021a849694f29b8f *linuxmint-22-cinnamon-64bit.iso
78a2438346cfe69a1779b0ac3fc05499f8dc7202959d597dd724a07475bc6930 *linuxmint-22-mate-64bit.iso
55e917b99206187564029476f421b98f5a8a0b6e54c49ff6a4cb39dcfeb4bd80 *linuxmint-22-xfce-64bit.iso
```

导致完整性验证失败：

```
→  linuxmint sha256sum -c sha256sum.txt
linuxmint-22-cinnamon-64bit.iso: FAILED
sha256sum: linuxmint-22-mate-64bit.iso: No such file or directory
linuxmint-22-mate-64bit.iso: FAILED open or read
sha256sum: linuxmint-22-xfce-64bit.iso: No such file or directory
linuxmint-22-xfce-64bit.iso: FAILED open or read
sha256sum: WARNING: 2 listed files could not be read
sha256sum: WARNING: 1 computed checksum did NOT match
```

身份验证同样失败：

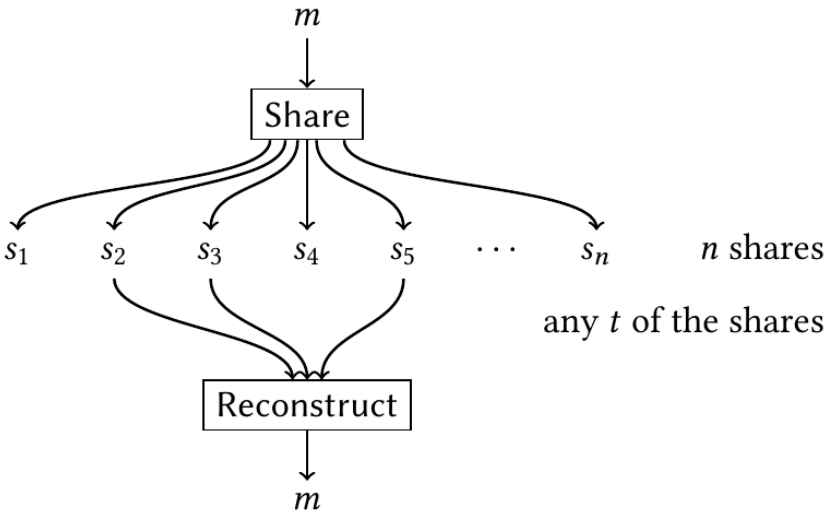
```
→  linuxmint gpg --verify sha256sum.txt.gpg sha256sum.txt
gpg: Signature made Tue 23 Jul 2024 02:03:50 AM CST
gpg:                using RSA key 27DEB15644C6B3CF3BD7D291300F846BA25BAE09
gpg: BAD signature from "Linux Mint ISO Signing Key <root@linuxmint.com>" [unknown]
```

目录

应用 3：秘密共享（Secret Sharing）

俄罗斯的核武器系统密码保存在总统手中，国防部也保存一份。当最高层作出发动核打击决定时，总统和国防部长分别通过不同的通讯网，将两组不同的密码传送到总参作战部电脑控制中心，经过运算形成一组有 12 位数字的第三套预发密码，再由特种通讯系统通过特殊频率传递给核潜艇指挥官和导弹发射基地，指挥官再按照程序输入密码，完成操作。

应用 3：(t, n)-门限秘密共享

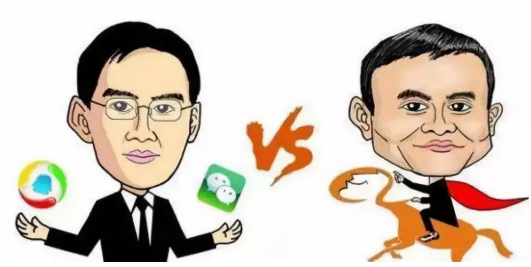


消息 m 被拆分为 n 份交给 n 个人，只有当其中至少 t 个人同意时，才能共同恢复原始消息 m。

目录

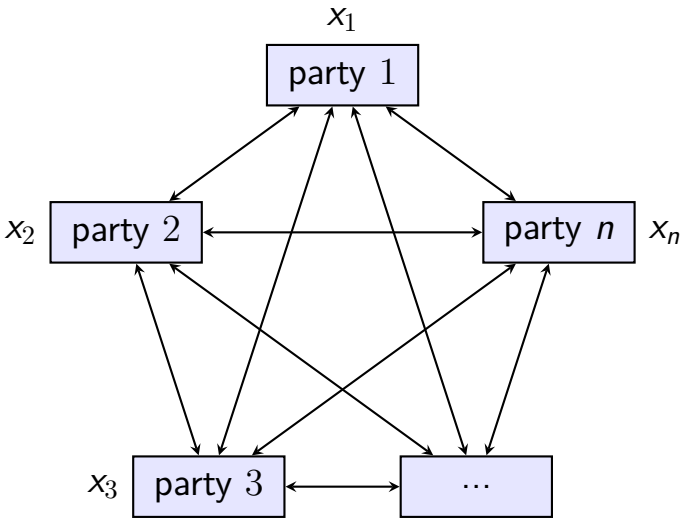
应用 4：百万富翁问题与安全多方计算

两个富翁在不泄漏个人财产具体数额的前提下，如何比较谁更富有[1]？



[1]Yao A C. Protocols for secure computations[C]// Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science, 1982.

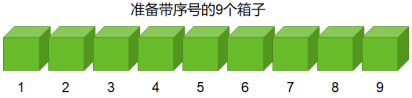
应用 4：安全多方计算的一般形式



$$(y_1, \ldots, y_n) = F(x_1, \ldots, x_n)$$

应用 4：百万富翁问题的一种通俗解法

- 假定富翁 Alice 和 Bob 的财富值 x, y 取值范围为 $\{1, \ldots, 9\}$（以 $x = 3, y = 7$ 为例）。
- 第一步：Alice 准备带序号 $1 \sim 9$ 的 9 个箱子。



- 第二步：Alice 在箱子内分别放入苹果和香蕉。如果箱子序号小于自己的财富值 x，则放入苹果；否则放入香蕉。

- 然后，Alice 将带序号的 9 个箱子密封后交给 Bob。

应用 4：百万富翁问题的一种通俗解法

- 第三步：Bob 收到带序号的箱子后，挑选序号与自己财富值 y 相等的箱子，然后撕掉序号，扔掉其他箱子。

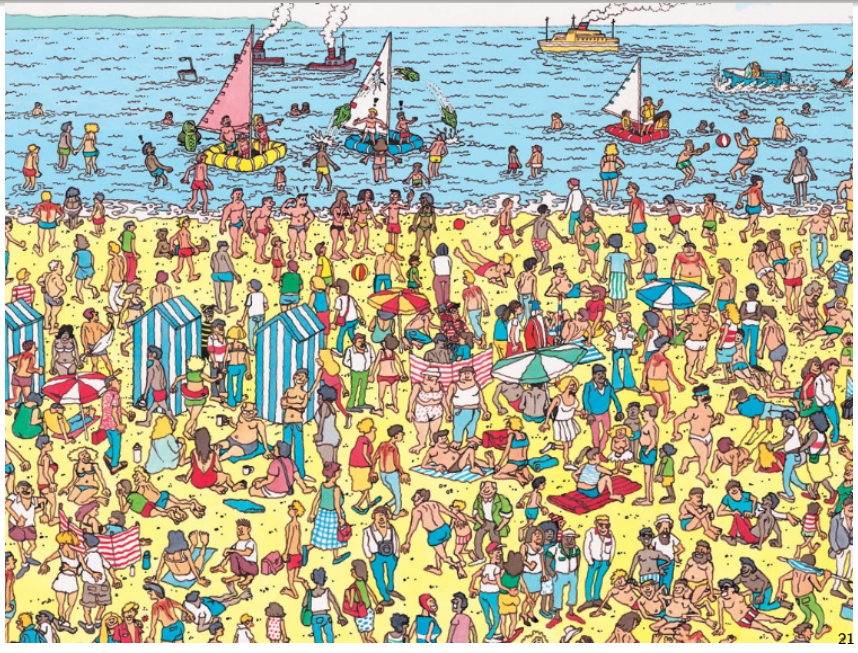
- 第四步：Bob 当着 Alice 的面打开选中的箱子，如果是香蕉，则 $y \geq x$；如果是苹果则 $x > y$。

- 虽然 Alice 和 Bob 都看到箱子里放的是香蕉（MPC 计算结果），但由于 Alice 不知道箱子序号，所以 Alice 不知道 Bob 选的是第几个箱子，即 Alice 不知道 Bob 的财富 y；
- Bob 不知道序号 $1 \sim 6$ 的 6 个箱子里从第几个箱子开始由苹果变成香蕉，即 Bob 不知道 Alice 的财富 x。

目录

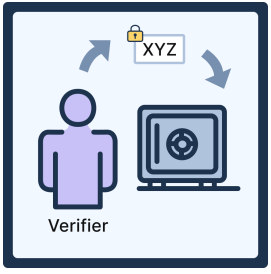
应用 5：零知识证明——寻找瓦利

瓦利

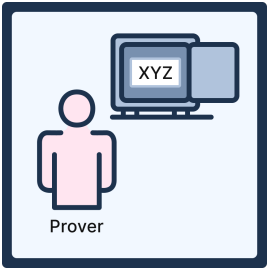


应用 5：零知识证明——成员证明问题

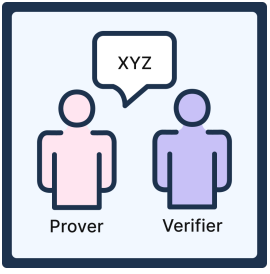
- 问题：你遇到一个不认识的人，但她声称也是你所在团队的成员，怎样做才可以信任她？
- 幸运的是，你的团队有一个保险箱，只有你的团队成员知道保险箱密码，可以打开保险箱。



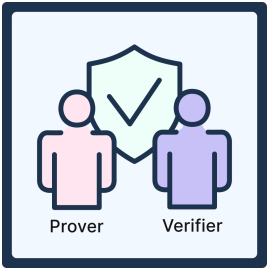
1. 验证者写一条秘密信息并放入锁定的保险箱中



2. 符合要求的证明者有密码，能打开保险箱



3. 证明者记下保险箱中的秘密信息并交给验证者



4. 验证者确信证明者真的知道密码，因此可以信任

应用 5：零知识证明——核裁军谈判

- 问题：一个国家的核武库属于国家最高机密，两个国家进行谈判后决定削减核弹头数量分别到一个约定的具体数目。
- 几年后，两个国家都声称核弹头数量已经削减到了约定数量。如何使一个国家相信另一个国家确实削减到了约定数量？

ARTICLE

doi:10.1038/nature13457

A zero-knowledge protocol for nuclear warhead verification

Alexander Glaser[1], Boaz Barak[2] & Robert J. Goldston[3]

ARTICLE

Received 27 Feb 2016 | Accepted 12 Aug 2016 | Published 20 Sep 2016

DOI: 10.1038/ncomms12890 OPEN

A physical zero-knowledge object-comparison system for nuclear warhead verification

Sébastien Philippe[1], Robert J. Goldston[2], Alexander Glaser[1] & Francesco d'Errico[3,4]

本章小结

1. 加密通信
2. 消息认证与数字签名
3. 秘密分享
4. 安全多方计算
5. 零知识证明