| | | | | | |
|---|---|---|---|---|---|
| Saal: Simulacron-3 | 11:15 | 00:30 | Day: 3 | Track: Science | nA |

Title: **Crypto Dawn**

Subtitle: A To Do list for Cyptographic Research and Implementations

Speaker: **ruedi**

**Short:** *Crypto seems to be the last line of defence in a wired world. "We mustimplement it, actively research it." (Eduard Snowden). So let us at least discuss some To Do things. How we can eliminate weak crypto algorithms from the last millennium from our daily protocols? How can we deal with the standardisation mess in the field of elliptic curves cryptography? Which protocols and algorithms are needed in a post quantum world? How "opportunistic" should we encrypt the masses? Could we provide a "moral, philosophical and technical commitment to enforce and defend our liberties" Eduard Snowden has ask us for?*

**Long:** Crypto Dawn: A To Do list for Cyptographic Research and Implementations Crypto seems to be the last line of defence in a wired world. "We must implement it, actively research it." (Eduard Snowden). So let us at least discuss some To Do things. - How we can eliminate weak crypto algorithms from the last millennium from our daily protocols? - How can we deal with the standardisation mess in the field of elliptic curves cryptography? - Which protocols and algorithms are needed in a post quantum world? - How "opportunistic" should we encrypt the masses? Could we provide a "moral, philosophical and technical commitment to enforce and defend our liberties" Eduard Snowden has ask us for?