Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

IT Security Research @ BHF: Hot Topics

Prof. Dr. Eric Dubuis

- Research Institute for Security in the Information Society RISIS

E-Voting…

«Egal, welches Wahlsystem man hat, es ist manipulierbar»

Andreas Gröflin

To counteract we…

- … we devise e-voting protocols and publish its specification

CHVote System Specification

Version 1.2

Rolf Haenni, Reto E. Koenig, Philipp Locher, Eric Dubuis
{rolf.haenni,reto.koenig,philipp.locher,eric.dubuis}@bfh.ch

August 7, 2017

Bern University of Applied Sciences
CH-2501 Biel, Switzerland

To counteract we…

- … we devise e-voting protocols and publish its specification

CHVote System Specification

Algorithm: GenShuffle$(\mathbf{e}, pk)$

Input: ElGamal encryptions $\mathbf{e} = (e_1, \ldots, e_N)$, $e_i \in \mathbb{G}_q^2$
Encryption key $pk \in \mathbb{G}_q$

$\psi \leftarrow$ GenPermutation(N) // $\psi = (j_1, \ldots, j_N) \in \Psi_N$, see Alg. 7.41

for $i = 1, \ldots, N$ **do**

  $(e'_i, r'_i) \leftarrow$ GenReEncryption(e_i, pk) // see Alg. 7.42

$\mathbf{e}' \leftarrow (e'_{j_1}, \ldots, e'_{j_N})$

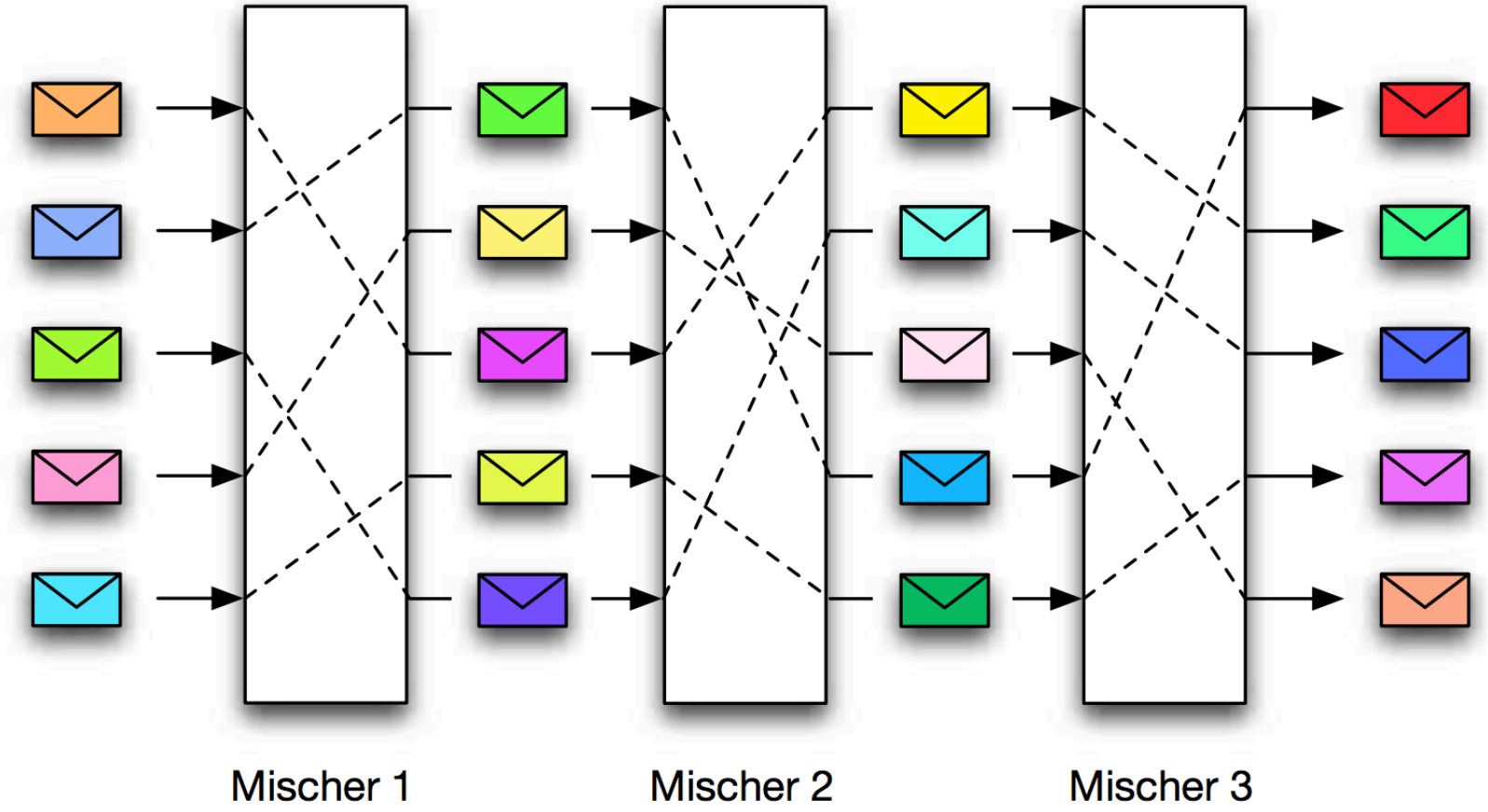
$\mathbf{r}' \leftarrow (r'_1, \ldots, r'_N)$

return $(\mathbf{e}', \mathbf{r}', \psi)$ // $\mathbf{e}' \in (\mathbb{G}_q^2)^N$, $\mathbf{r}' \in \mathbb{Z}_q^N$, $\psi \in \Psi_N$

Algorithm 7.40: Generates a random permutation $\psi \in \Psi_N$ and uses it to shuffle a given list $\mathbf{e} = (e_1, \ldots, e_N)$ of ElGamal encryptions $e_i = (a_i, b_i) \in \mathbb{G}_q^2$. With $\Psi_N = \{(j_1, \ldots, j_N) : j_i \in \{1, \ldots, N\}, j_{i_1} \neq j_{i_2}, \forall i_1 \neq i_2\}$ we denote the set of all $N!$ possible permutations of the indices $\{1, \ldots, N\}$.

To counteract we…

- … we devise e-voting protocols and publish its specification



To counteract we…

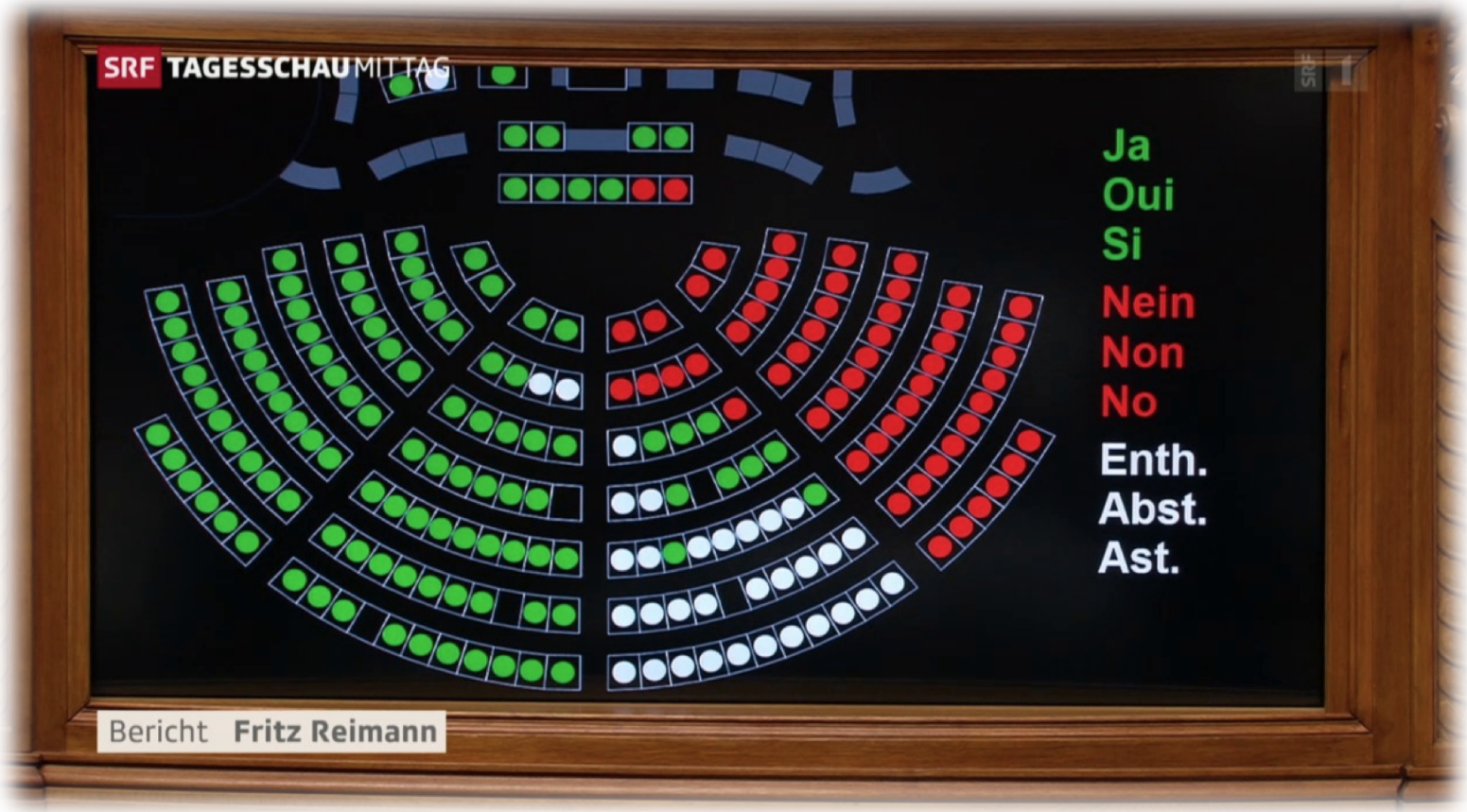
- … we promote individual verification

To counteract we…

- … we promote individual verification

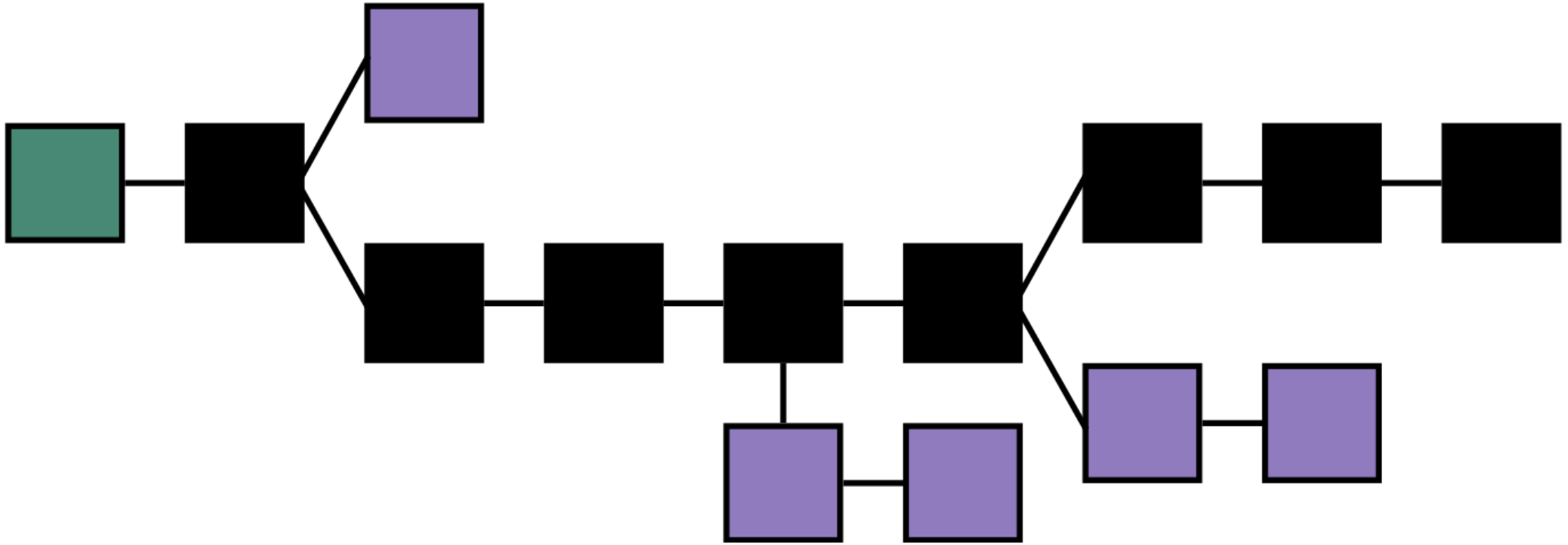
To counteract we…

- … we promote universal verification …



To counteract we…

- … and search for linking the public bulletin board to a blockchain



… and we cooperate with …

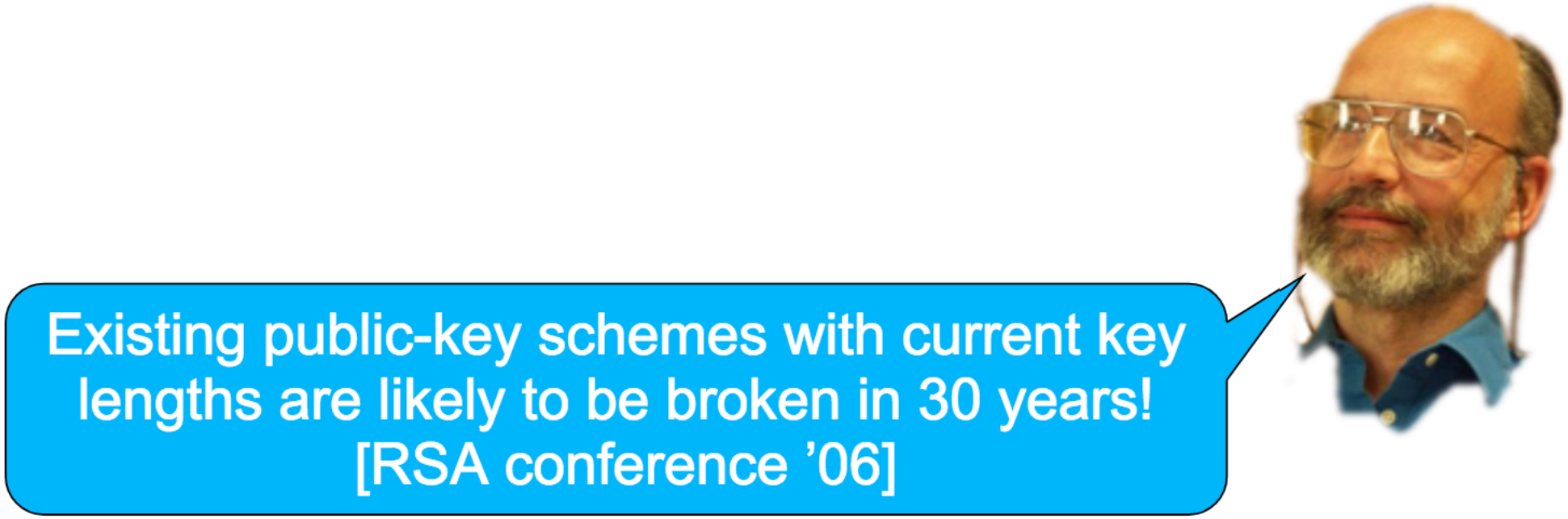
- … the State of Geneva
- … Swiss Post
- … others

Challenges…

- … the secure platform problem

Challenges…

- … ever lasting privacy

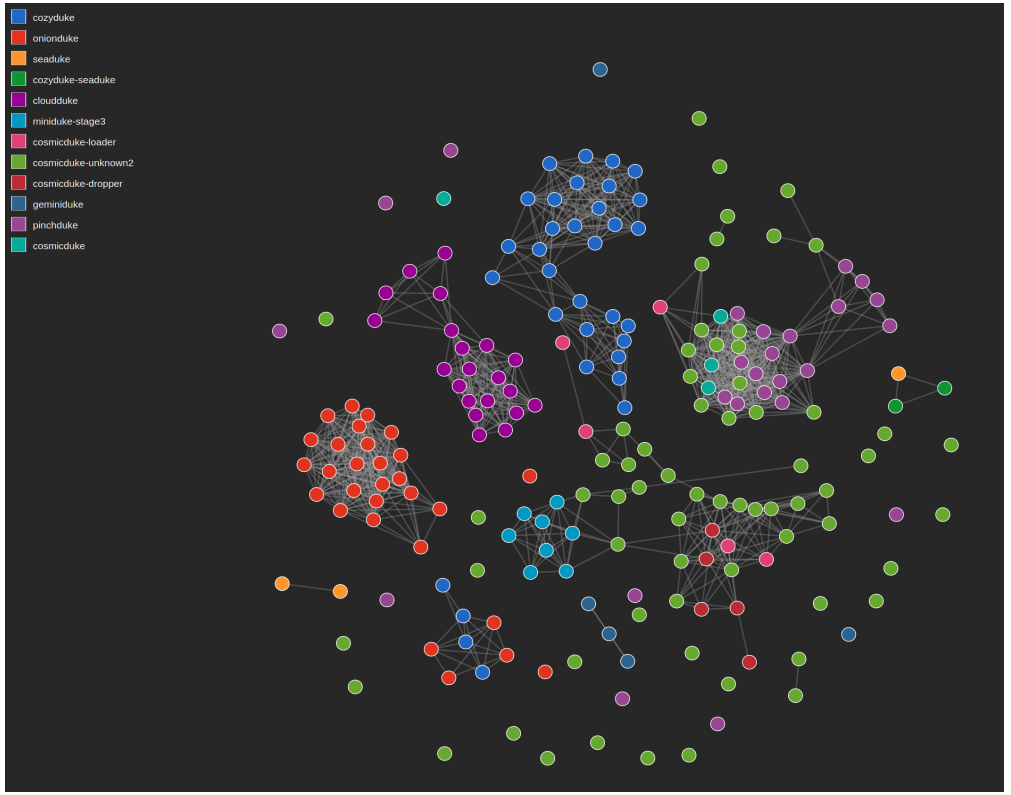


Cyber Forensics and Intelligence Lab...

Cyber Forensics & Intelligence Lab

Prof. Dr. Endre Bangerter (BFH and GovCERT.ch / MELANI)

Prof. Dr. Bruce Nikkel (BFH and UBS)



Research focus areas:

- Code based threat intelligence
- Memory analysis and introspection techniques
- Malware forensics
- Digital forensics (disk, network, memory, IoT)
- Finance industry specific cybercrime

Thank you

Prof. Dr. Eric Dubuis
Berner Fachhochschule
RISIS
2501 Biel
Switzerland