Fair Mutual Authentication

Jacek Cichoń, Mirosław Kutyłowski, Krzysztof Majcher

[1] Department of Fundamentals of Computer Science, Wrocław University of Science and Technology, Wrocław, Poland

SECRYPT 2021

Mutual authentication

Goal of mutual authentication

- Alice and Bob communicate online
- Alice wants to know that she **really** talks with Bob
- Bob wants to know that he **really** talks with Alice

J. Cichoń,
M. Kutyłowski,
K. Majcher

Protocol example

Authentication via a shared key K

1. Bob chooses random N_B and sends it to Alice,
2. Alice chooses random N_A and sends it and $P_A = \mathrm{Hash}(K, N_A \| N_B, \text{“Alice, Bob”})$ to Bob,
3. Bob computes $P'_A = \mathrm{Hash}(K, N_A \| N_B, \text{“Alice”}, \text{“Bob”})$ and aborts if $P'_A \neq P_A$,
4. Bob returns $P_B = \mathrm{Hash}(K, N_A \| N_B, \text{“Bob”}, \text{“Alice”})$ to Alice,
5. Alice computes $P'_B = \mathrm{Hash}(K, N_A \| N_B, \text{“Bob”}, \text{“Alice”})$ aborts if $P'_B \neq P_B$,
6. Alice, Bob: accept if not aborted

Tracing Problem

- **at step 3 Bob learns that he is talking with Alice**
- **until step 5 Alice learns nothing**

GDPR and privacy-by-design

Mutual authentication protocol turns to be an effective tracing tool.

The location of a physical person is under protection.

No-tracing possible – by design!

Markov Fair Mutual Authentication

Idea

- Alice and Bob exchange the authenticating information bit-by-bit
- **some bits sent are false** at random moments
- ... nevertheless **no partner has a substantial information advantage at any moment**

False bits versus cryptanalysis

!!! an observer has no idea which bits are correct

$\Longrightarrow$ like for Learning Parity With Errors: cryptanalysis becomes substantially harder

J. Cichoń,
M. Kutyłowski,
K. Majcher

Details

Let $P_A = a_1, a_2, a_3, \ldots, a_n$ and $P_B = b_1, b_2, b_3, \ldots, b_n$,
$p \in [0, 1]$ – a probability parameter

Round i

let Δ_i be the difference between the number of erroneous bits sent by Alice and Bob.

- if $\Delta_i = -1$, then Alice sends a_i,
- if $\Delta_i = 0$ or $\Delta_i = 1$, then Alice sends a_i with probability p and $\neg a_i$ with probability $1 - p$,
- if $\Delta_i > 1$, then Alice enters the `failure` state and from now on sends random bits.

J. Cichoń,
M. Kutyłowski,
K. Majcher

Features

GDPR: no tracing, $\approx$ same amount of personal personal data bits exchanged in each direction regardless of protocol run

lightweight: due to erroneous bits, relatively weak hash function can be used as well as small number of bits exchanged. IoT friendly!

Markov chain

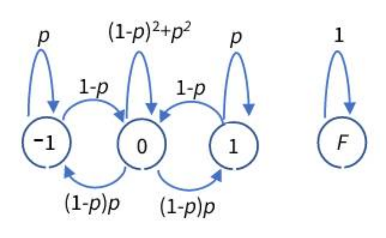
Differences as a Markov chain

Stochastic process $\{\Delta_i\}_i$ examined

> $\Delta_i =$ the difference between the numbers of correct authentication bits sent by Bob and Alice up to round i

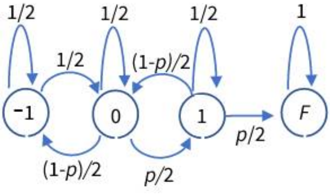
It is a Markov chain with states $-1, 0, 1$ and a failure state F.

Fair Execution



- optimal choice for parameter p is $\frac{2}{3}$
- process very quickly converges to the stationary distribution: $\pi = (\frac{2}{7}, \frac{3}{7}, \frac{2}{7}, 0)$
- expected fraction of incorrect bits $\approx \frac{1}{4}$
- incorrect bits well distributed

Execution with a Party Impersonating Bob



- The most critical moment from the point of information leakage is a visit in the state -1. In this case, Alice must send the correct bit.
- the number of visits of the state -1 during a protocol execution is a random variable Z
- it should be small!
- for for $p = \frac{2}{3}$:

$$E[Z]\frac{3}{2}, \quad Var[Z] = \frac{27}{4}$$

J. Cichoń,
M. Kutyłowski,
K. Majcher

Thank you for your attention!

Acknowledgments

Thanks for Łukasz Krzywiecki for bringing attention to the problem