A leakage-resilient MAC

Joachim Schipper

supervised by Eike Kiltz and Krzysztof Pietrzak

May 4th, 2010

Side-channel attacks

Side-channel attacks (SCAs) are attacks that exploit (physical) properties of the *implementation*, e.g. power use. Even the best smart cards and similar devices are vulnerable to SCAs.

- Practitioners have tried to solve this
  - Ad-hoc
  - Only partially succesful
- Leakage-resilient cryptography is the theoretical approach
  - Inspired by provable security
  - Requires a good model of what SCAs can do

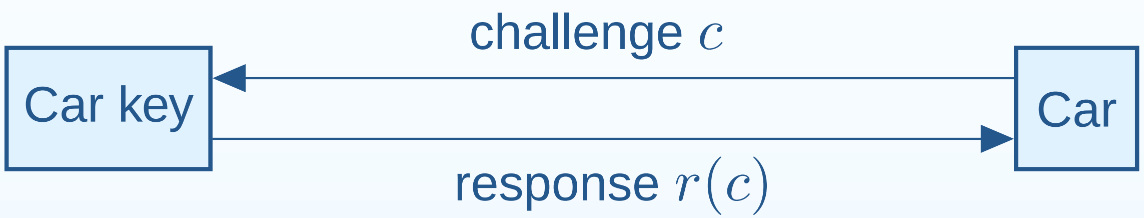
Leakage-resilient cryptography

We use the model of continuous leakage proposed by Dziembowski and Pietrzak [DP08, Pie09].

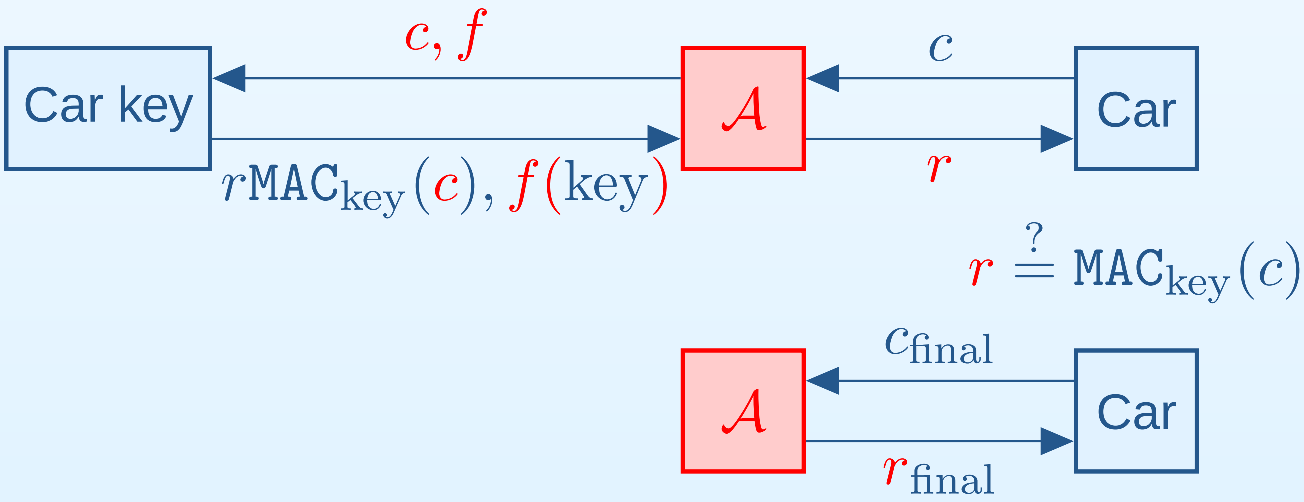
- Mostly equal to the standard model…
- …but the adversary can supply a *leakage function* with each input, and receives the output of this function with the output.
  - this function must produce λ bits of output, where λ depends on the (quality of) implementation
  - only computation leaks information
  - this function must be efficient

Leakage-resilient authentication

Inspired by the power analysis of KeeLoq [EKM$^+$08].

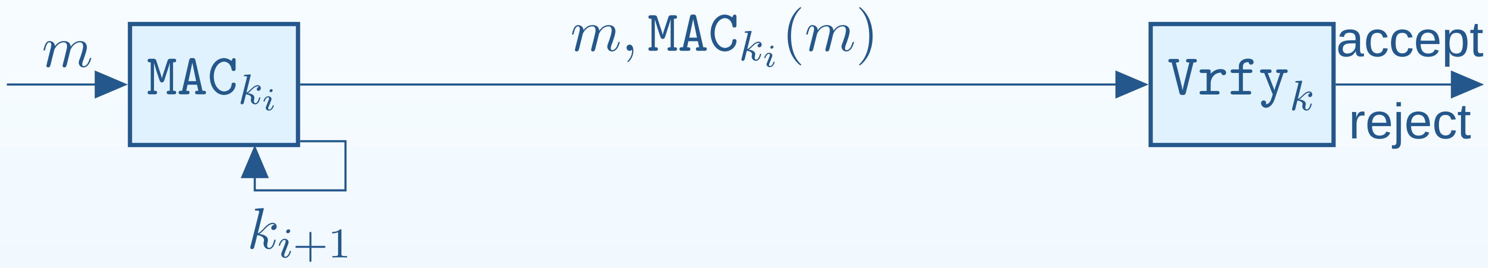


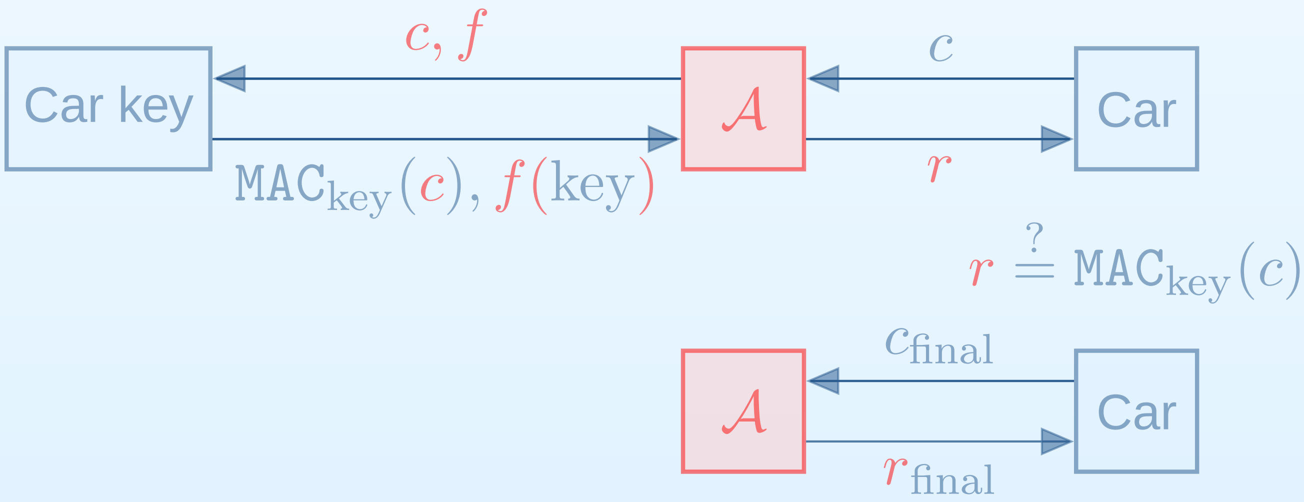
The adversary has temporary access and wins if r_{final} is valid. The classical solution is a MAC. Of course, we need leakage-resilience.



Stateful MACs

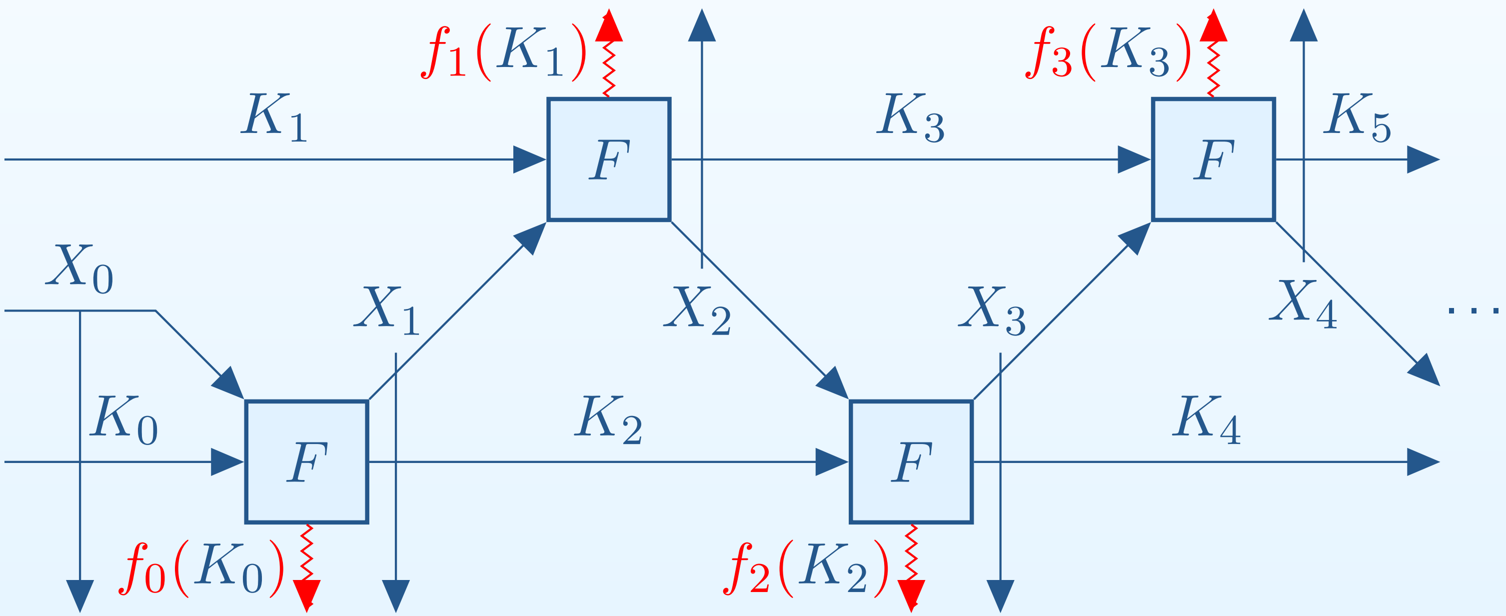
Problem: if we use the same key each time, it will eventually completely leak. So we need a *stateful* MAC.





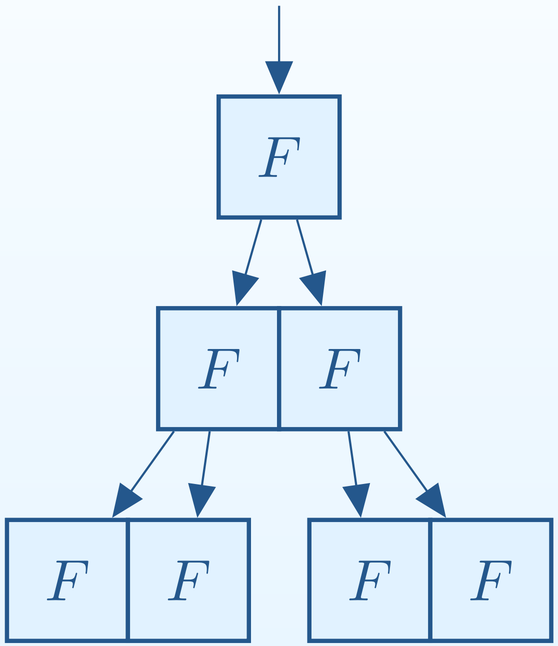
A leakage-resilient stream cipher [Pie09]

Stream cipher: X_i is pseudorandom given $X_0, X_1, \ldots, X_{i-1}$.
Leakage-resilient stream cipher: X_i is pseudorandom given $X_0, X_1, X_2, \ldots, X_{i-1}$ and the leakage $f_0(K_0^+), f_1(K_1^+), \ldots, f_{i-1}(K_{i-1}^+)$ from these rounds.



Tree-based leakage-resilient stream cipher

We are working on this.



The authenticating side performs a depth-first search on the tree.The verifier only needs to perform $O(\log(\#\text{queries}))$ calculations to calculate any output.

Questions?

References

[DP08] Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *FOCS*, pages 293–302. IEEE Computer Society, 2008.

[EKM+08] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani. On the power of power analysis in the real world: A complete break of the KeeLoq code hopping scheme. In David Wagner, editor, *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 203–220. Springer, 2008.

[Pie09] Krzysztof Pietrzak. A leakage-resilient mode of operation. In Antoine Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 462–482. Springer, 2009.