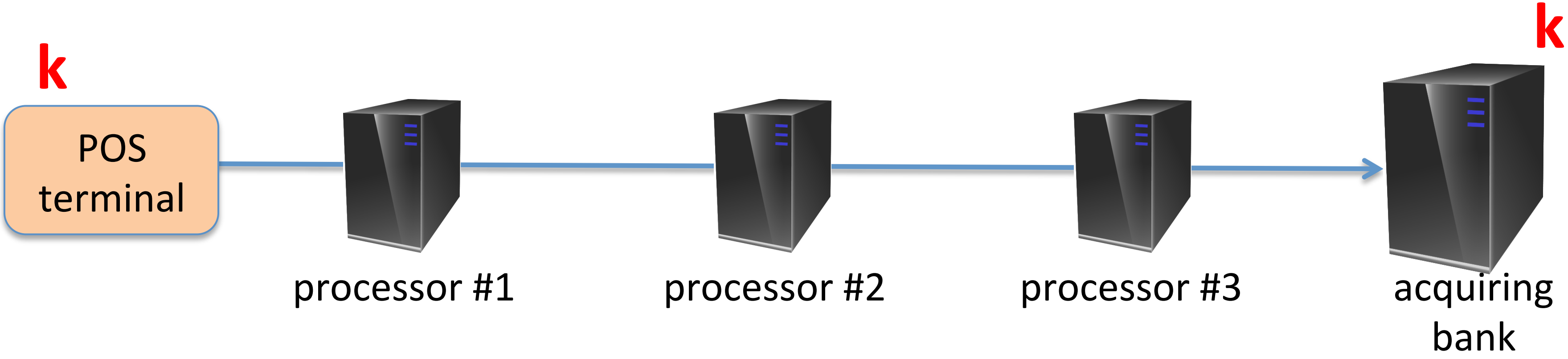
Odds and ends

Format preserving encryption

Encrypting credit card numbers

Credit card format: **bbbb bbnn nnnn nnnc** (≈ 42 bits)



Goal: end-to-end encryption

Intermediate processors expect to see a credit card number

⇒ encrypted credit card should look like a credit card

Format preserving encryption (FPE)

This segment: given $0 < s \leq 2^n$, build a PRP on $\{0,\dots,s-1\}$

from a secure PRF **$F: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$** (e.g. AES)

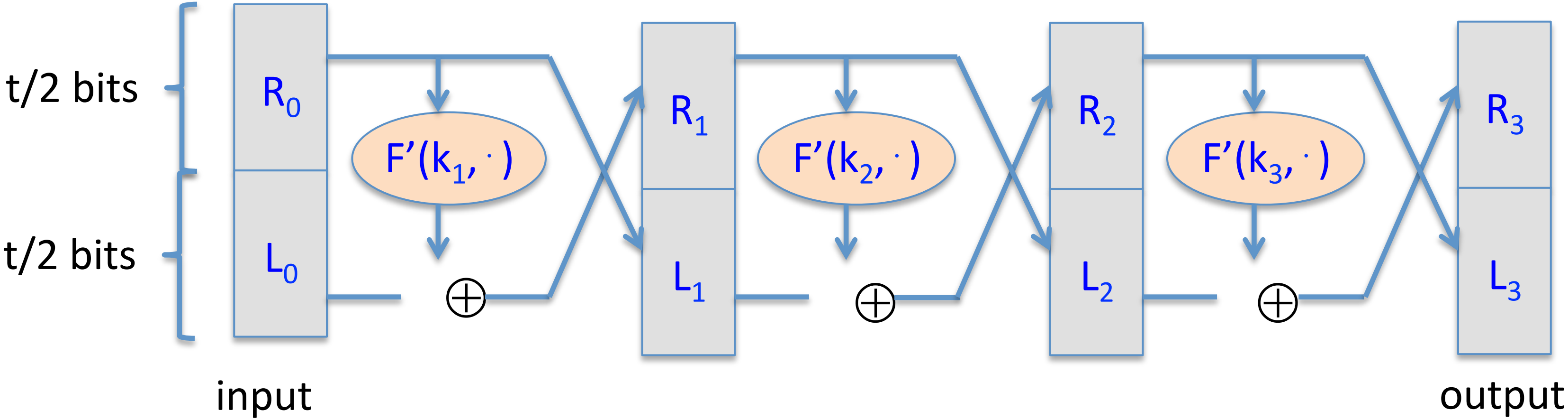
Then to encrypt a credit card number: (s = total # credit cards)

1. map given CC# to $\{0,\dots,s-1\}$
2. apply PRP to get an output in $\{0,\dots,s-1\}$
3. map output back a to CC#

Step 1: from $\{0,1\}^n$ to $\{0,1\}^t$ (t<n)

Want PRP on $\{0,\ldots,s-1\}$. Let t be such that $2^{t-1} < s \le 2^t$.

Method: Luby-Rackoff with $F': K \times \{0,1\}^{t/2} \longrightarrow \{0,1\}^{t/2}$ (truncate F)



(better to use 7 rounds a la Patarin, Crypto'03)

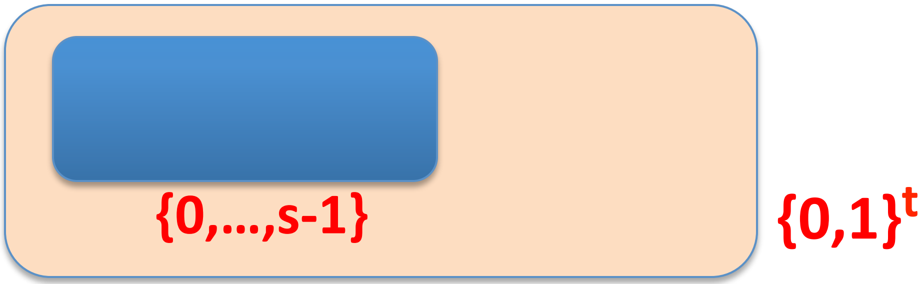
Step 2: from $\{0,1\}^t$ to $\{0,\ldots,s\text{-}1\}$

Given PRP $(E,D): K \times \{0,1\}^t \longrightarrow \{0,1\}^t$

we build $(E',D'): K \times \{0,\ldots,s\text{-}1\} \longrightarrow \{0,\ldots,s\text{-}1\}$

$E'(k, x)$: on input $x \in \{0,\ldots,s\text{-}1\}$ do:

$y \longleftarrow x$; do { $y \longleftarrow E(k, y)$ } until $y \in \{0,\ldots,s\text{-}1\}$; output y



Expected # iterations:

Security

Step 2 is tight: $\forall A \quad \exists B: \quad \mathrm{PRP}_{adv}[A,E] = \mathrm{PRP}_{adv}[B,E']$

Intuition: $\forall$ sets $Y \subseteq X$, applying the transformation to a random perm. $\pi: X \longrightarrow X$

gives a random perm. $\pi': Y \longrightarrow Y$

Step 1: same security as Luby-Rackoff construction

(actually using analysis of Patarin, Crypto'03)

note: no integrity

Further reading

- Cryptographic Extraction and Key Derivation: The HKDF Scheme.
  H. Krawczyk, Crypto 2010

- Deterministic Authenticated-Encryption:
  A Provable-Security Treatment of the Keywrap Problem.
  P. Rogaway, T. Shrimption, Eurocrypt 2006

- A Parallelizable Enciphering Mode. S. Halevi, P. Rogaway, CT-RSA 2004

- Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. P. Rogaway, Asiacrypt 2004

- How to Encipher Messages on a Small Domain:
  Deterministic Encryption and the Thorp Shuffle.
  B. Morris, P. Rogaway, T. Stegers, Crypto 2009

End of Segment