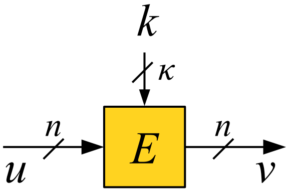
Encryption based on Card Shuffle

Jooyoung Lee

Faculty of Mathematics and Statistics, Sejong University

October 3, 2015

Block Cipher

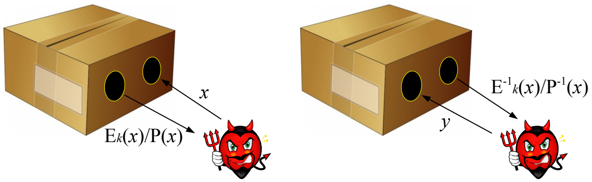


- A block cipher is a function

$$E : \{0,1\}^{\kappa} \times \{0,1\}^{n} \to \{0,1\}^{n}$$

  such that for all $k \in \{0,1\}^{\kappa}$ the mapping $E(k,\cdot)$ is a permutation on $\{0,1\}^{n}$.
- Most block ciphers such as DES and AES operate on $64 \sim 128$ bit blocks

Security of Encryption Scheme: Indistinguishability

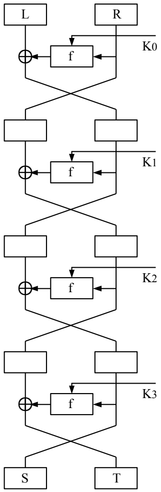


- An adversary makes a certain number of oracle queries to the black box in two different directions
  - Ideal World: a truly random permutation P
  - Real World: a keyed block cipher E_k for a random secret key k
- The adversarial goal is to tell apart the two worlds
- If the distinguishing advantage is small, this block cipher is said to be secure

Encryption of Data of Small Size

- If we need to encrypt all the credit card numbers in the data base as the ciphertexts of the same format
- Data size is too small
- Using AES? A new block cipher?

Feistel Network



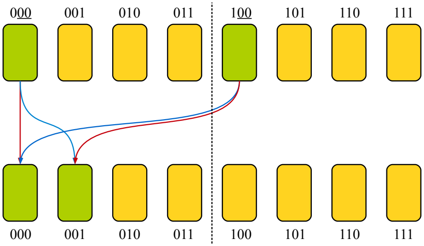
- Even in the case the round function is perfectly secure (namely, truly random):
- the entire permutation is secure only up to $2^{\frac{n}{2}}$ queries for a sufficient number of rounds, where n is the block size
- Not suitable if the data size n is too small

Card Shuffle

1. The final position of a card of a certain position(=plaintext) is viewed as the encryption of the plaintext
2. Card shuffle is a Markov process
   - Mixing time=number of rounds
3. Should be oblivious: one should be able to trace the trajectory of a card without attending to lots of other cards

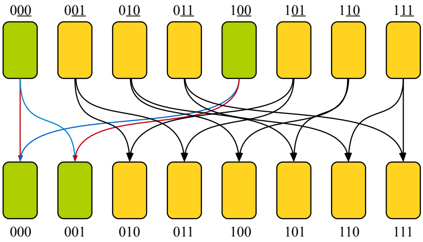
Thorp Shuffle

- 3-bit values represent the positions of the cards
- The cards at $0**$ and $1**$ are matched
- They come together, while swapped or not according to the evaluation of a round function at "$**$"
- This process is a single round of a blockcipher structure
- Secure up to $2^n/n$ queries (Crypto 2009) for $O(n^2)$ rounds



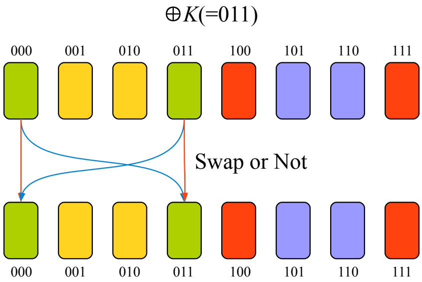
Thorp Shuffle

- 3-bit values represent the positions of the cards
- The cards at $0**$ and $1**$ are matched
- They come together, while swapped or not according to the evaluation of a round function at "$**$"
- This process is a single round of a blockcipher structure
- Secure up to $2^n/n$ queries (Crypto 2009) for $O(n^2)$ rounds

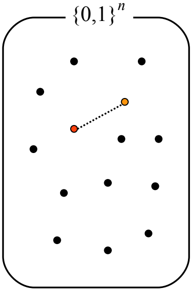


Swap-or-Not Shuffle (Crypto 2012)

- A round key $K(\neq 0)$ is chosen uniformly at random from $\{0, 1\}^3$
- The cards at positions x and $x \oplus K$ are matched
- They are swapped or not according to the evaluation of a round function at "$\max\{x, x \oplus K\}$"
- Secure up to $(1 - \epsilon)2^n$ queries for any $\epsilon > 0$ for $O(n)$ rounds

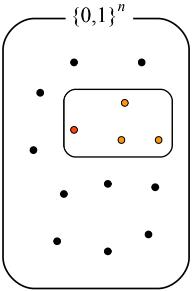


Another View of the SN Shuffle



1. For each element, a distinct element is chosen uniformly at random.
   - A single pairing might determine all the other pairings.
2. A random permutation is applied to the pair of size two.
   - The random permutations applied to the pairs are all independent.

New Construction: Partition-and-Mix



1. For each element, $D-1$ distinct elements are chosen uniformly at random ($D \geq 2$).
   - A single block might determine all the other blocks.
2. A random permutation is applied to the set of size D.
   - The random permutations applied to the blocks are all independent.

New Construction: Partition-and-Mix

Definition

Let N, $D \geq 2$ be integers such that $D|N$, $\varepsilon > 0$ and let

$$\mathcal{B}_K = \{B_K^i\}_{i=1,\ldots,\frac{N}{D}}$$

be a keyed partition of $[N] = \{0, 1, \ldots, N-1\}$ into blocks of size D . Then $\mathcal{B}_K$ is called ε-almost D-uniform if for any set U of size D

$$\Pr\left[K \leftarrow_{\$} \mathcal{K} : U \in \mathcal{B}_K\right] \leq \frac{1+\varepsilon}{\binom{N-1}{D-1}}.$$

Remark

If a partition of $[N]$ into blocks of size D is chosen uniformly at random from the set of all possible partitions, then for any set U of size D

$$\Pr\left[U \in \mathcal{B}_K\right] = \frac{1}{\binom{N-1}{D-1}}.$$

Security of the Partition-and-Mix

Theorem

Let PM^r be the r-round partition-and-mix shuffle on $[N]$ defined by an ε-almost D-uniform keyed partition. Then

$$\mathbf{Adv}^{\mathrm{cca}}_{\mathrm{PM}^r}(q) \leq \frac{4\,(1+\varepsilon)^{\frac{r}{4}}\, N^{\frac{r}{4}+\frac{1}{2}}}{(r-4)D^{\frac{r}{4}}(N-q)^{\frac{r}{4}-1}}.$$

Result

The number of rounds is reduced by a factor of $\log_2 \frac{D}{1+\varepsilon}$ for a same level of security.

Efficient Implementation of the Partition-and-Mix

Problem

How to implement a (almost) D-uniform random partition for a given D?

Definition

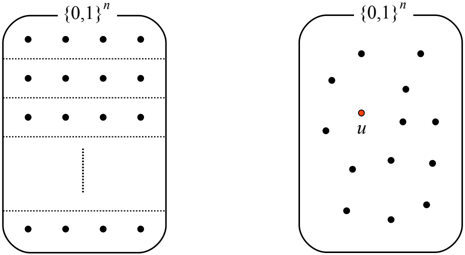
A family of permutations on N elements is perfect D-wise independent if it acts uniformly on tuples of D elements.

Example

A keyed permutation family g such that $g_{K_1,K_2}(v) = K_1 \cdot v + K_2$ is perfect 2-wise independent.

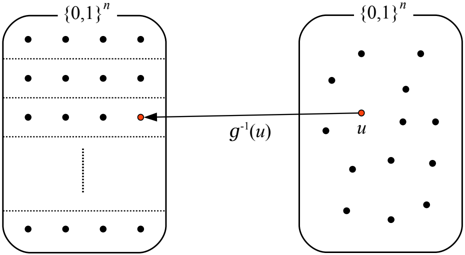
- multiplication and addition are done in $GF(2^n)$ and K_1 is nonzero

Partition: Using D-wise Independent Permutation Family



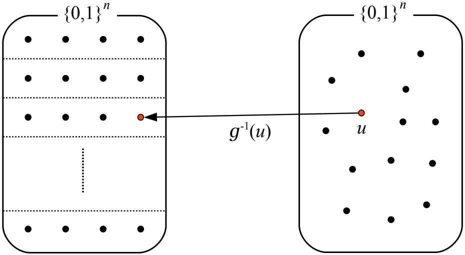
1. Each element u is mapped by g^{-1}, where g is (implicitly keyed) D-wise independent permutation.
2. $g^{-1}(u)$ is contained in a certain block V in a fixed partition of $\{0, 1\}^n$.
3. $U = g(V)$ is defined as a random block containing u.

Partition: Using D-wise Independent Permutation Family



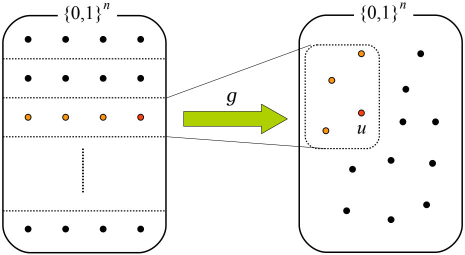
1. Each element u is mapped by g^{-1}, where g is (implicitly keyed) D-wise independent permutation.
2. $g^{-1}(u)$ is contained in a certain block V in a fixed partition of $\{0,1\}^n$.
3. $U = g(V)$ is defined as a random block containing u.

Partition: Using D-wise Independent Permutation Family



1. Each element u is mapped by g^{-1}, where g is (implicitly keyed) D-wise independent permutation.
2. $g^{-1}(u)$ is contained in a certain block V in a fixed partition of $\{0, 1\}^n$.
3. $U = g(V)$ is defined as a random block containing u.

Partition: Using D-wise Independent Permutation Family



1. Each element u is mapped by g^{-1}, where g is (implicitly keyed) D-wise independent permutation.
2. $g^{-1}(u)$ is contained in a certain block V in a fixed partition of $\{0, 1\}^n$.
3. $U = g(V)$ is defined as a random block containing u.

Example: 2-wise Independent Permutation Family

- Suppse that the fixed partition is

$$\mathcal{V} = \{\{v, v+1\} : v \in \{0,1\}^n\}$$

- A random permutation is defined as

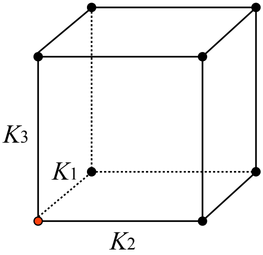
$$g_{K_1,K_2}(v) = K_1 \cdot v + K_2$$

- Given $u \in \{0,1\}^n$, $g^{-1}_{K_1,K_2}(u) = K_1^{-1} \cdot (u + K_2)$
- Then u is paired with

$$g\left(g^{-1}_{K_1,K_2}(u) + 1\right) = K_1 \cdot \left(K_1^{-1} \cdot (u + K_2) + 1\right) + K_2 = u + K_1$$

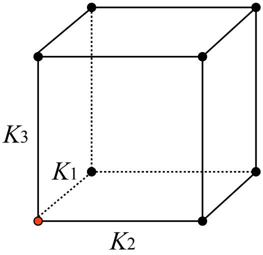
- Same as used in the swap-or-not shuffle
- Negative result: no nontrivial subgroups of S_n ($n \geq 25$) which are 4-wise independent

Partition: Using Hamming Codes (3-dimension)



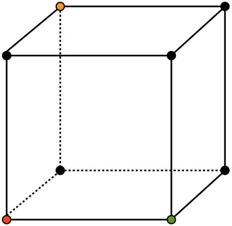
1. For each round, linearly independent round keys K_1, K_2, K_3 are chosen uniformly at random
2. Set $\{0,1\}^n$ is decomposed into the cosets of $\langle K_1, K_2, K_3 \rangle$
3. Two vertices on a diagonal line are randomly chosen for each coset
4. Each coset is again decomposed into two blocks around the vertices

Partition: Using Hamming Codes (3-dimension)



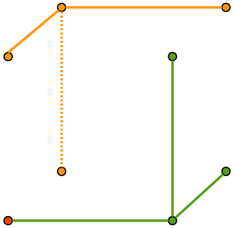
1. For each round, linearly independent round keys K_1, K_2, K_3 are chosen uniformly at random
2. Set $\{0,1\}^n$ is decomposed into the cosets of $\langle K_1, K_2, K_3 \rangle$
3. Two vertices on a diagonal line are randomly chosen for each coset
4. Each coset is again decomposed into two blocks around the vertices

Partition: Using Hamming Codes (3-dimension)



1. For each round, linearly independent round keys K_1, K_2, K_3 are chosen uniformly at random
2. Set $\{0, 1\}^n$ is decomposed into the cosets of $\langle K_1, K_2, K_3 \rangle$
3. Two vertices on a diagonal line are randomly chosen for each coset
4. Each coset is again decomposed into two blocks around the vertices

Partition: Using Hamming Codes (3-dimension)



1. For each round, linearly independent round keys K_1, K_2, K_3 are chosen uniformly at random
2. Set $\{0,1\}^n$ is decomposed into the cosets of $\langle K_1, K_2, K_3 \rangle$
3. Two vertices on a diagonal line are randomly chosen for each coset
4. Each coset is again decomposed into two blocks around the vertices

Partition: Using Hamming Codes

This approach is extended to the use of binary perfect $[2^s - 1, 2^s - s - 1, 3]$-Hamming codes (for $D = 2^s$)

1. Choose uniformly at random a set of linearly independent keys $K_1, \ldots, K_{D-1} \in \{0, 1\}^n$.
   - The entire domain $\{0, 1\}^n$ is partitioned into the cosets of $V = \langle K_1, \ldots, K_{D-1} \rangle$.
2. Choose a random representative **a** for each coset, and define a bijection from $\{0, 1\}^{D-1}$ to the coset by mapping
$$(e_1, \ldots, e_{D-1}) \in \{0, 1\}^{D-1} \mapsto \mathbf{a} + e_1 K_1 + \cdots + e_{D-1} K_{D-1}.$$
3. Using the Hamming code $\mathcal{C}_s$, one obtains a partition of each coset as
$$\{0, 1\}^{D-1} = \bigcup_{c \in \mathcal{C}_s} \{c + e : \mathbf{wt}(e) \leq 1\}.$$

Partition: Using Hamming Codes

This approach is extended to the use of binary perfect $[2^s - 1, 2^s - s - 1, 3]$-Hamming codes (for $D = 2^s$)

1. Choose uniformly at random a set of linearly independent keys $K_1, \ldots, K_{D-1} \in \{0,1\}^n$.
   - The entire domain $\{0,1\}^n$ is partitioned into the cosets of $V = \langle K_1, \ldots, K_{D-1} \rangle$.
2. Choose a random representative **a** for each coset, and define a bijection from $\{0,1\}^{D-1}$ to the coset by mapping

$$(e_1, \ldots, e_{D-1}) \in \{0,1\}^{D-1} \mapsto \mathbf{a} + e_1 K_1 + \cdots + e_{D-1} K_{D-1}.$$

3. Using the Hamming code $\mathcal{C}_s$, one obtains a partition of each coset as

$$\{0,1\}^{D-1} = \bigcup_{c \in \mathcal{C}_s} \{c + e : \mathbf{wt}(e) \leq 1\}.$$

Partition: Using Hamming Codes

This approach is extended to the use of binary perfect $[2^s - 1, 2^s - s - 1, 3]$-Hamming codes (for $D = 2^s$)

1. Choose uniformly at random a set of linearly independent keys $K_1, \ldots, K_{D-1} \in \{0,1\}^n$.
   - The entire domain $\{0,1\}^n$ is partitioned into the cosets of $V = \langle K_1, \ldots, K_{D-1} \rangle$.
2. Choose a random representative **a** for each coset, and define a bijection from $\{0,1\}^{D-1}$ to the coset by mapping

$$(e_1, \ldots, e_{D-1}) \in \{0,1\}^{D-1} \mapsto \mathbf{a} + e_1 K_1 + \cdots + e_{D-1} K_{D-1}.$$

3. Using the Hamming code $\mathcal{C}_s$, one obtains a partition of each coset as

$$\{0,1\}^{D-1} = \bigcup_{c \in \mathcal{C}_s} \{c + e : \mathbf{wt}(e) \leq 1\}.$$

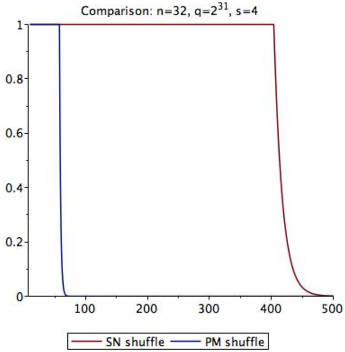
Partition: Using Hamming Codes

This approach is extended to the use of binary perfect $[2^s - 1, 2^s - s - 1, 3]$-Hamming codes (for $D = 2^s$)

1. Choose uniformly at random a set of linearly independent keys $K_1, \ldots, K_{D-1} \in \{0,1\}^n$.
   - The entire domain $\{0,1\}^n$ is partitioned into the cosets of $V = \langle K_1, \ldots, K_{D-1} \rangle$.
2. Choose a random representative **a** for each coset, and define a bijection from $\{0,1\}^{D-1}$ to the coset by mapping
$$(e_1, \ldots, e_{D-1}) \in \{0,1\}^{D-1} \mapsto \mathbf{a} + e_1 K_1 + \cdots + e_{D-1} K_{D-1}.$$
3. Using the Hamming code $\mathcal{C}_s$, one obtains a partition of each coset as
$$\{0,1\}^{D-1} = \bigcup_{c \in \mathcal{C}_s} \{c + e : \mathbf{wt}(e) \leq 1\}.$$

Partition: Using Hamming Codes

- The resulting keyed partition is $\frac{2^D}{2^n}$-almost D-uniform



- This example of the partition-and-mix uses a keyed 4-bit S-boxes

Conclusion

Results

- Generalized the swap-or-not shuffle
- Number of rounds reduced
- Can be viewed as a new block cipher structure
- Particularly useful for format preserving encryption

Future Research Problems

- Finding (almost) uniform keyed partitions that allow efficient implementation
- Efficient construction of very small permutations (operating on a small number of bits)

Thank You!