The End of Encryption based on Card Shuffling

Serge Vaudenay

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

http://lasec.epfl.ch/

Every Day I’m Shuffling

An Enciphering Scheme Based on a Card Shuffle

Tung Hoang, Morris, Rogaway; Crypto 2012

proc $E_{KF}(X)$
key: $K_1, \ldots, K_r, F_1, \ldots, F_r$
for $i = 1$ to r **do**
    $X' \leftarrow K_i \oplus X$
    $\hat{X} \leftarrow \max(X, X')$
    if $F_i(\hat{X}) = 1$ then $X \leftarrow X'$
end for
return X

secure when *KF* is uniformly distributed

An Enciphering Scheme Based on a Card Shuffle

A Proposed Instance

proc $E_{KL}(X)$

key: $K_1, \ldots, K_r, L_1, \ldots, L_r$

for $i = 1$ to r **do**

  $X' \leftarrow K_i \oplus X$

  $\hat{X} \leftarrow \max(X, X')$

  if $L_i \cdot \hat{X} = 1$ then $X \leftarrow X'$

end for

return X

An Enciphering Scheme Based on a Card Shuffle

A Proposed Instance

proc $E_{KL}(X)$
key: $K_1, \ldots, K_r, L_1, \ldots, L_r$

```
for i = 1 to r do
    X' ← K_i ⊕ X
    X̂ ← max(X, X')
    if L_i · X̂ = 1 then X ← X'
end for
return X
```

- in round i, let j be the highest index such that $(K_i)_j = 1$
- $\hat{X} = \max(X, X \oplus K_i) = X \oplus \overline{\mathrm{bit}_j(X)} K_i$
- $X_{\text{new}} = X \oplus (L_i \cdot \hat{X}) K_i$
- these functions have algebraic degree 1 in X
- encryption is linear!

An Enciphering Scheme Based on a Card Shuffle

A Proposed Instance

proc $E_{KL}(X)$
key: $K_1, \ldots, K_r, L_1, \ldots, L_r$

```
for i = 1 to r do
    X' ← K_i ⊕ X
    X̂ ← max(X, X')
    if L_i · X̂ = 1 then X ← X'
end for
return X
```

- in round i, let j be the highest index such that $(K_i)_j = 1$
- $\hat{X} = \max(X, X \oplus K_i) = X \oplus \overline{\mathrm{bit}_j(X)} K_i$
- $X_{\mathrm{new}} = X \oplus (L_i \cdot \hat{X}) K_i$
- these functions have algebraic degree 1 in X
- encryption is linear!

An Enciphering Scheme Based on a Card Shuffle

A Proposed Instance

proc $E_{KL}(X)$

key: $K_1, \ldots, K_r, L_1, \ldots, L_r$

for $i = 1$ to r **do**
  $X' \leftarrow K_i \oplus X$
  $\hat{X} \leftarrow \max(X, X')$
  if $L_i \cdot \hat{X} = 1$ then $X \leftarrow X'$
end for
return X

- in round i, let j be the highest index such that $(K_i)_j = 1$
- $\hat{X} = \max(X, X \oplus K_i) = X \oplus \overline{\text{bit}_j(X)} K_i$
- $X_{\text{new}} = X \oplus (L_i \cdot \hat{X}) K_i$
- these functions have algebraic degree 1 in X
- encryption is linear!

An Enciphering Scheme Based on a Card Shuffle

A Proposed Instance

proc $E_{KL}(X)$
key: $K_1, \ldots, K_r, L_1, \ldots, L_r$
1: **for** $i = 1$ to r **do**
2: $X' \leftarrow K_i \oplus X$
3: $\hat{X} \leftarrow \max(X, X')$
4: if $L_i \cdot \hat{X} = 1$ then $X \leftarrow X'$
5: **end for**
6: return X

- in round i, let j be the highest index such that $(K_i)_j = 1$
- $\hat{X} = \max(X, X \oplus K_i) = X \oplus \overline{\text{bit}_j(X)} K_i$
- $X_{\text{new}} = X \oplus (L_i \cdot \hat{X}) K_i$
- these functions have algebraic degree 1 in X
- encryption is linear!

An Enciphering Scheme Based on a Card Shuffle

A Proposed Instance

proc $E_{KL}(X)$

key: $K_1, \ldots, K_r, L_1, \ldots, L_r$

```
for i = 1 to r do
    X' ← K_i ⊕ X
    X̂ ← max(X, X')
    if L_i · X̂ = 1 then X ← X'
end for
return X
```

- in round i, let j be the highest index such that $(K_i)_j = 1$
- $\hat{X} = \max(X, X \oplus K_i) = X \oplus \overline{\mathrm{bit}_j(X)} K_i$
- $X_{\mathrm{new}} = X \oplus (L_i \cdot \hat{X}) K_i$
- these functions have algebraic degree 1 in X
- encryption is linear!

The End of Encryption based on Card Shuffling?

- certainly not: still secure if *KF* is uniform
- open questions:
  could it be secure with a distribution over a smaller set?
  could we replace max by another symmetric function?

```
proc E_KL(X)
key: K_1, ..., K_r, L_1, ..., L_r
for i = 1 to r do
    X' ← K_i ⊕ X
    X̂ ← (X + X') mod 2^ℓ
    if L_i · X̂ = 1 then X ← X'
end for
return X
```

an idea by Henri Gilbert:

$$F_i(x) = \text{majority}\left(L_i \cdot x, L'_i \cdot x, L''_i \cdot x\right)$$

(this is has degree 2)

The End of Encryption based on Card Shuffling?

- certainly not: still secure if *KF* is uniform
- open questions:

  could it be secure with a distribution over a smaller set?

  could we replace max by another symmetric function?

proc $E_{KL}(X)$

key: $K_1, \ldots, K_r, L_1, \ldots, L_r$

1: **for** $i = 1$ to r **do**

2: $X' \leftarrow K_i \oplus X$

3: $\hat{X} \leftarrow (X + X') \bmod 2^{\ell}$

4: if $L_i \cdot \hat{X} = 1$ then $X \leftarrow X'$

5: **end for**

6: return X

an idea by Henri Gilbert:

$F_i(x) = \text{majority}\left(L_i \cdot x, L'_i \cdot x, L''_i \cdot x\right)$

(this is has degree 2)

The End of Encryption based on Card Shuffling?

- certainly not: still secure if *KF* is uniform
- open questions:
  could it be secure with a distribution over a smaller set?
  could we replace max by another symmetric function?

proc $E_{KL}(X)$
key: $K_1, \ldots, K_r, L_1, \ldots, L_r$

for $i = 1$ to r **do**
    $X' \leftarrow K_i \oplus X$
    $\hat{X} \leftarrow (X + X') \bmod 2^\ell$
    if $L_i \cdot \hat{X} = 1$ then $X \leftarrow X'$
end for
return X

an idea by Henri Gilbert:

$$F_i(x) = \text{majority}\left(L_i \cdot x, L'_i \cdot x, L''_i \cdot x\right)$$

(this is has degree 2)

The End of Encryption based on Card Shuffling?

- certainly not: still secure if *KF* is uniform
- open questions:
  could it be secure with a distribution over a smaller set?
  could we replace max by another symmetric function?

proc $E_{KL}(X)$

key: $K_1, \ldots, K_r, L_1, \ldots, L_r$

```
for i = 1 to r do
    X' ← K_i ⊕ X
    X̂ ← (X + X') mod 2^ℓ
    if L_i · X̂ = 1 then X ← X'
end for
return X
```

an idea by Henri Gilbert:

$$F_i(x) = \text{majority}\left(L_i \cdot x, L_i' \cdot x, L_i'' \cdot x\right)$$

(this is has degree 2)