UNIVERSITÄT ZU LÜBECK

Steganography Based on Pattern Languages

Sebastian Berndt Rüdiger Reischuk

Institut für Theoretische Informatik, Universität zu Lübeck

IM FOCUS DAS LEBEN

And now for something completely different!

- Cryptography: Hide the content of a message

And now for something completely different!

- Cryptography: Hide the content of a message
- Steganography: Hide that a message is transferred

Sometimes, cryptography is not enough

Overview

Steganography

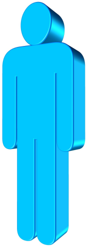
Pattern Languages

The stegosystem

Conclusion

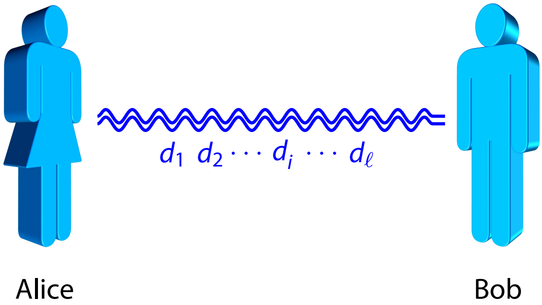
The Prisoners' Problem (not the Dilemma)

Alice

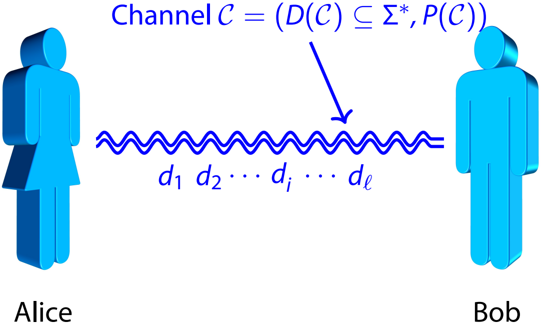


Bob

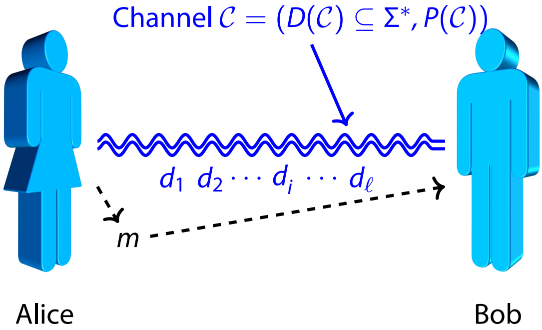
The Prisoners' Problem (not the Dilemma)



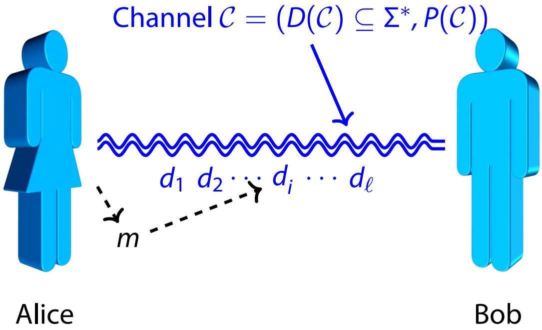
The Prisoners' Problem (not the Dilemma)



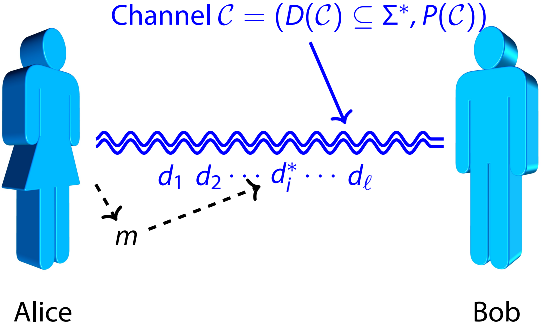
The Prisoners' Problem (not the Dilemma)



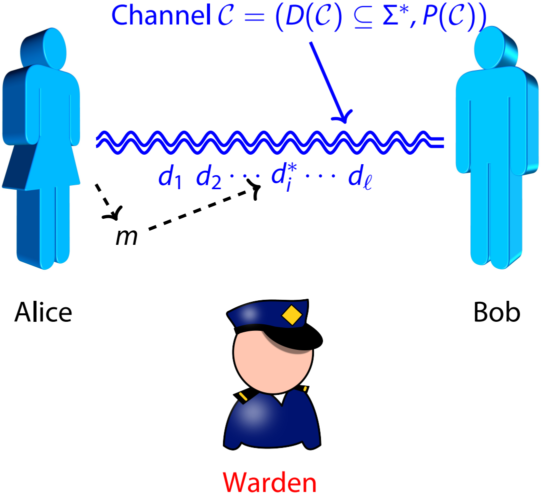
The Prisoners' Problem (not the Dilemma)



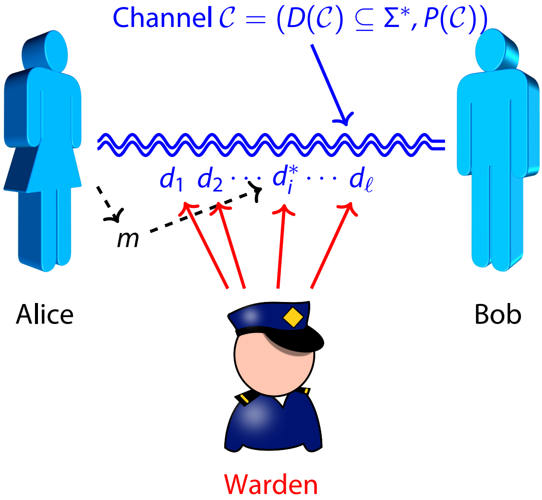
The Prisoners' Problem (not the Dilemma)



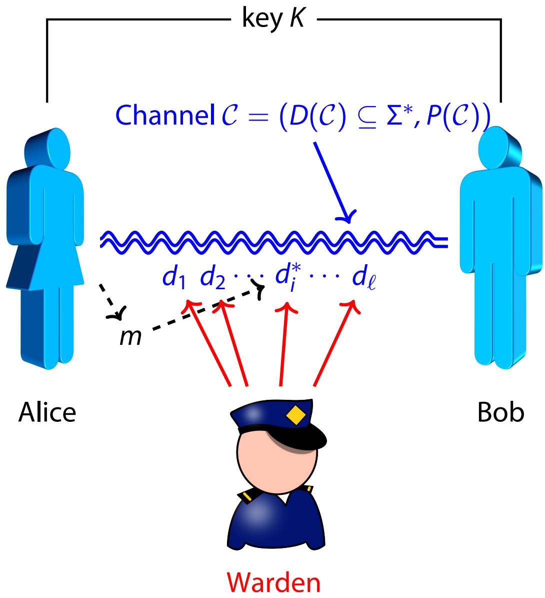
The Prisoners' Problem (not the Dilemma)



The Prisoners' Problem (not the Dilemma)



The Prisoners' Problem (not the Dilemma)



Requirements of a stegosystem

- Warden should not be able to distinguish d_i from d_i^* (*Security*)

Requirements of a stegosystem

- Warden should not be able to distinguish d_i from d_i^* (*Security*)
- Bob should be able to reconstruct the message (*Reliability*)

Requirements of a stegosystem

- Warden should not be able to distinguish d_i from d_i^* (*Security*)
- Bob should be able to reconstruct the message (*Reliability*)
- Alice and Bob should be computational feasible (*Efficiency*)

Requirements of a stegosystem

- Warden should not be able to distinguish d_i from d_i^* (*Security*)
- Bob should be able to reconstruct the message (*Reliability*)
- Alice and Bob should be computational feasible (*Efficiency*)
- Alice should get high transmission rate (*Rate-efficiency*)

Requirements of a stegosystem

- Warden should not be able to distinguish d_i from d_i^* (*Security*)
- Bob should be able to reconstruct the message (*Reliability*)
- Alice and Bob should be computational feasible (*Efficiency*)
- Alice should get high transmission rate (*Rate-efficiency*)
  (Bounded by the *channel-entropy* n)

Requirements of a stegosystem

- Warden should not be able to distinguish d_i from d_i^* (*Security*)
- Bob should be able to reconstruct the message (*Reliability*)
- Alice and Bob should be computational feasible (*Efficiency*)
- Alice should get high transmission rate (*Rate-efficiency*)
  (Bounded by the *channel-entropy* n)
- Should work for as much channels as possible (*Applicability*)

Universality

Universal

- Stegosystem is *universal* if it works for *every* channel.

Universality

Universal

- Stegosystem is *universal* if it works for *every* channel.
- Such secure systems can embed only $\log n$ bits.

Universality

Universal

- Stegosystem is *universal* if it works for *every* channel.
- Such secure systems can embed only $\log n$ bits. Practical systems embed $\sqrt{n}$.

Universality

Universal

- Stegosystem is *universal* if it works for *every* channel.
- Such secure systems can embed only $\log n$ bits. Practical systems embed $\sqrt{n}$.
- To embed `HELLO WORLD`, we need length $\geq 2^{88} \approx 3 \cdot 10^{12}\text{PB} \approx 10^{10} \cdot \mathit{Space}(\text{Facebook})$.

Universality

Universal

- Stegosystem is *universal* if it works for *every* channel.
- Such secure systems can embed only $\log n$ bits. Practical systems embed $\sqrt{n}$.
- To embed `HELLO WORLD`, we need length $\geq 2^{88} \approx 3 \cdot 10^{12}$PB $\approx 10^{10} \cdot \mathit{Space}(\text{Facebook})$.

Task

Be more specific: Develop stegosystem for large channel-family $\mathcal{F}$!

Previous Work

LB on Rate	UB on Rate	Channels	Authors
$\log(n)$	✗	universal	Hopper et al. (2002)

Previous Work

LB on Rate	UB on Rate	Channels	Authors
$\log(n)$	✗	universal	Hopper et al. (2002)
$\log(n)$	$\log(n)$	universal	Dedić et al. (2005)

Previous Work

LB on Rate	UB on Rate	Channels	Authors
$\log(n)$	✗	universal	Hopper et al. (2002)
$\log(n)$	$\log(n)$	universal	Dedić et al. (2005)
$\sqrt{n}$	✗	Monomials	Liśkiewicz et al. (2011)

Previous Work

LB on Rate	UB on Rate	Channels	Authors
$\log(n)$	✗	universal	Hopper et al. (2002)
$\log(n)$	$\log(n)$	universal	Dedić et al. (2005)
$\sqrt{n}$	✗	Monomials	Liśkiewicz et al. (2011)
$\sqrt{n}$	✗	Pattern Languages	this work

Previous Work

LB on Rate	UB on Rate	Channels	Authors
$\log(n)$	✗	universal	Hopper et al. (2002)
$\log(n)$	$\log(n)$	universal	Dedić et al. (2005)
$\sqrt{n}$	✗	Monomials	Liśkiewicz et al. (2011)
$\sqrt{n}$	✗	Pattern Languages	this work

Much more systems exist, but none are provable secure!

Monomials

$X = ?01?1?$
001010
001011
001110
001111
101010
101011
101110
101111

Monomials

$X = ?01?1?$
001010
001011
001110
001111
101010
101011
101110
101111

$D(\mathcal{C})$

Monomials

$X = ?01?1?$
001010
001011
001110
001111
101010
101011
101110
101111

$D(\mathcal{C})$

The system

1. Partition the positions of X into blocks $B_1, \ldots, B_b$ via PRP
2. Replace the different ?'s such that $\sum_{x \in B_i} x = m_i$

Monomials

$X = ?01?1?$
001010
001011
001110
001111
101010
101011
101110
101111

$\Big\}\, D(\mathcal{C})$

The system

1. Partition the positions of X into blocks $B_1, \ldots, B_b$ via PRP
2. Replace the different ?'s such that $\sum_{x \in B_i} x = m_i$

Restrictions

- Simplest non-trivial language

Monomials

$X = ?01?1?$
001010
001011
001110
001111
101010
101011
101110
101111

$D(\mathcal{C})$

The system

1. Partition the positions of X into blocks $B_1, \ldots, B_b$ via PRP
2. Replace the different ?'s such that $\sum_{x \in B_i} x = m_i$

Restrictions

- Simplest non-trivial language
- Simple cross product

Patterns

$\pi = x_1 01 x_2 1 x_1$
011
00110
0101
001010
...
1111010011111
...

Patterns

$\pi = x_1 01 x_2 1 x_1$
011
00110
0101
001010
...
111101001111
...

Advantages

- More realistic (forms, websites etc.)

Patterns

$\pi = x_1 01 x_2 1 x_1$
011
00110
0101
001010
...
11110100011111
...

Advantages

- More realistic (forms, websites etc.)
- Much larger class of languages

Pattern Channels

- $D(\mathcal{C}) \subseteq \mathrm{Lang}(\pi)$

$$d_1 \; d_2 \cdots \; d_i \cdots \; d_\ell \; \sim \mathrm{Lang}(\pi)$$

Pattern Channels

- $D(\mathcal{C}) \subseteq \mathrm{Lang}(\pi)$
- The pattern π is known (or can be learned)

$$d_1\ d_2 \cdots\ d_i \cdots\ d_\ell\ \sim \mathrm{Lang}(\pi)$$

Pattern Channels

- $D(\mathcal{C}) \subseteq \mathrm{Lang}(\pi)$
- The pattern π is known (or can be learned)
- The documents are of approximately same size

$$d_1\ d_2 \cdots\ d_i \cdots\ d_\ell \sim \mathrm{Lang}(\pi)$$

Pattern Channels

- $D(\mathcal{C}) \subseteq \mathrm{Lang}(\pi)$
- The pattern π is known (or can be learned)
- The documents are of approximately same size
- Substitutions of variables are independent

$$d_1 \ d_2 \cdots \ d_i \cdots \ d_\ell \ \sim \mathrm{Lang}(\pi)$$

The stegosystem

- Expand $\pi = x_1 0 1 x_2 1 x_1$ into $[\pi] = y_1 y_2 y_3 0 1 y_4 1 y_1 y_2 y_3$.

The stegosystem

- Expand $\pi = x_1 0 1 x_2 1 x_1$ into $[\pi] = y_1 y_2 y_3 0 1 y_4 1 y_1 y_2 y_3$.
- Use pseudo-random function F_K to partition $[\pi]$ in b Blocks

y_1

y_2

y_3

0

1

y_4

1

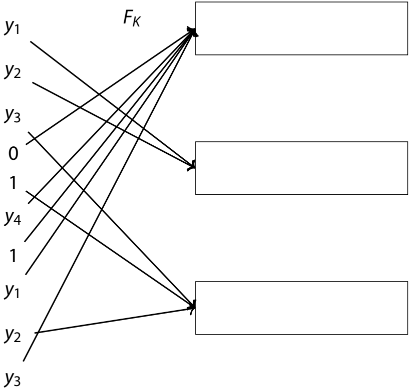
y_1

y_2

y_3

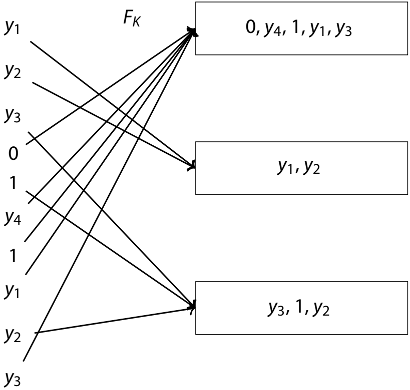
The stegosystem

- Expand $\pi = x_1 01 x_2 1 x_1$ into $[\pi] = y_1 y_2 y_3 01 y_4 1 y_1 y_2 y_3$.
- Use pseudo-random function F_K to partition $[\pi]$ in b Blocks



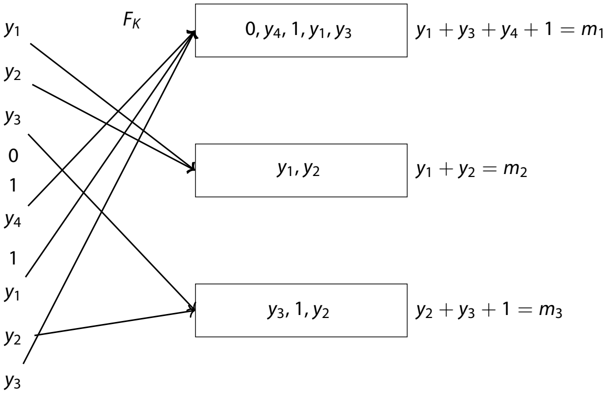
The stegosystem

- Expand $\pi = x_1 0 1 x_2 1 x_1$ into $[\pi] = y_1 y_2 y_3 0 1 y_4 1 y_1 y_2 y_3$.
- Use pseudo-random function F_K to partition $[\pi]$ in b Blocks



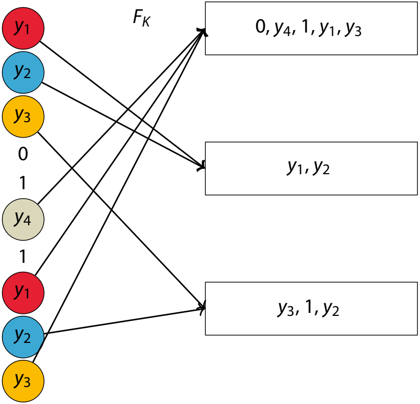
The stegosystem

- Expand $\pi = x_1 0 1 x_2 1 x_1$ into $[\pi] = y_1 y_2 y_3 0 1 y_4 1 y_1 y_2 y_3$.
- Use pseudo-random function F_K to partition $[\pi]$ in b Blocks



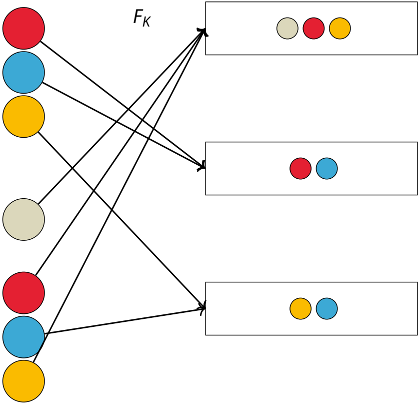
The stegosystem

- Expand $\pi = x_1 01 x_2 1 x_1$ into $[\pi] = y_1 y_2 y_3 01 y_4 1 y_1 y_2 y_3$.
- Use pseudo-random function F_K to partition $[\pi]$ in b Blocks

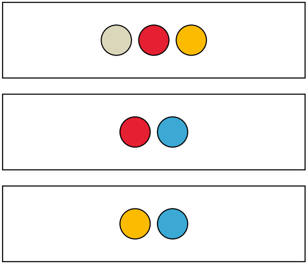


The stegosystem

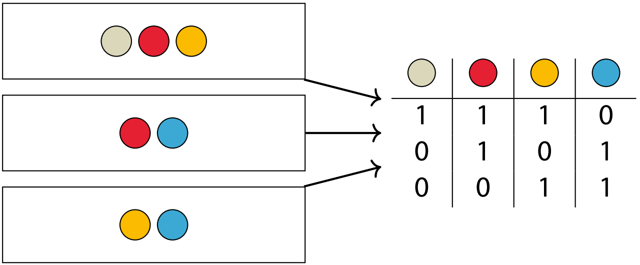
- Expand $\pi = x_1 01 x_2 1 x_1$ into $[\pi] = y_1 y_2 y_3 01 y_4 1 y_1 y_2 y_3$.
- Use pseudo-random function F_K to partition $[\pi]$ in b Blocks



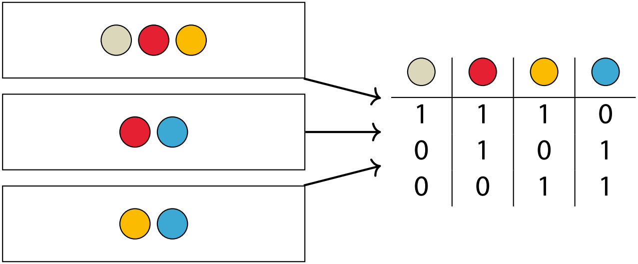
Coloured Balls into Bins



Coloured Balls into Bins

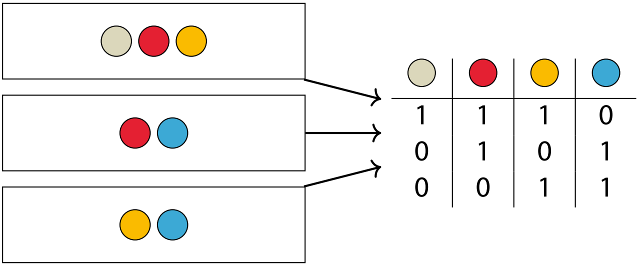


Coloured Balls into Bins



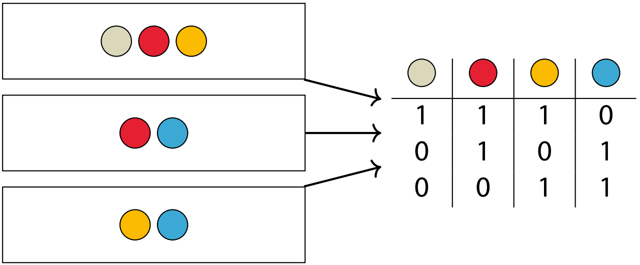
- Columns are independent

Coloured Balls into Bins



- Columns are independent
- Rows are *not* independent

Coloured Balls into Bins



1	1	1	0
0	1	0	1
0	0	1	1

- Columns are independent
- Rows are *not* independent

Theorem (Generalization of Poisson Approximation)

W.h.p. there are many colours such that the corresponding rows behave independently!

Some Useful Lemmata

Lemma

Let C be the coloured-balls-into-bin matrix with μ bins, where each colour appears at most ξ times and let X be a matrix of pairwise independent Poisson-distributed RVs.
For every predicate Q of arity l, let $\mathcal{E}_Q(X)$ be the probability that X has a subset of l columns $X_{z_1}, \ldots, X_{z_l}$ such that $Q(X_{z_1}, \ldots, X_{z_l})$ holds. Then:

$$\Pr[\mathcal{E}_Q(C)] \leq \frac{\Pr[\mathcal{E}_Q(X)]}{1 - 2\exp\left(-2\,\eta(l, n, \xi)\right)}.$$

Some Useful Lemmata

Lemma

Let C be the coloured-balls-into-bin matrix with μ bins, where each colour appears at most ξ times and let X be a matrix of pairwise independent Poisson-distributed RVs.
For every predicate Q of arity l, let $\mathcal{E}_Q(X)$ be the probability that X has a subset of l columns $X_{z_1}, \ldots, X_{z_l}$ such that $Q(X_{z_1}, \ldots, X_{z_l})$ holds. Then:

$$\Pr[\mathcal{E}_Q(C)] \le \frac{\Pr[\mathcal{E}_Q(X)]}{1 - 2\exp\left(-2\,\eta(l, n, \xi)\right)}.$$

Lemma

The matrix M with $m_{i,j} = x_{i,j} \bmod 2$ has full rank over $\mathbb{F}_2$ with probability at least $1 - \mu \cdot (4/5)^{\mu}$.

Some Useful Lemmata

Lemma

Let C be the coloured-balls-into-bin matrix with μ bins, where each colour appears at most ξ times and let X be a matrix of pairwise independent Poisson-distributed RVs.
For every predicate Q of arity l, let $\mathcal{E}_Q(X)$ be the probability that X has a subset of l columns $X_{z_1}, \ldots, X_{z_l}$ such that $Q(X_{z_1}, \ldots, X_{z_l})$ holds. Then:

$$\Pr[\mathcal{E}_Q(C)] \leq \frac{\Pr[\mathcal{E}_Q(X)]}{1 - 2\exp\left(-2\,\eta(l, n, \xi)\right)} .$$

Lemma

The matrix M with $m_{i,j} = x_{i,j} \bmod 2$ has full rank over $\mathbb{F}_2$ with probability at least $1 - \mu \cdot (4/5)^{\mu}$.

Corollary

If $n \geq b^2$, it holds that: $|\Pr[\mathcal{E}_Q(C)] - \Pr[\mathcal{E}_Q(X)]| \leq \exp(-n)$.

Open Questions

- Public-Key Scenario?

Open Questions

- Public-Key Scenario?
- Steganography for other families of languages ($D(\mathcal{C})$ described by automata, grammars, logics, . . .)?

Conclusion

Secure, rate-efficient steganography is possible on realistic channels!