TSINGHUA UNIVERSITY

A Cross Application Research to Block Cipher and Artificial Intelligence

Post P.HD. Lan Luo
Broadband Networks & Digital Media Lab
School of Information Science & Technology
Automation Dep. Tsinghua University

清華大學

TSINGHUA UNIVERSITY

分组密码与人工智能的交叉应用研究

罗 岚　博士后

宽带网数字媒体技术实验室

清华大学信息科学技术学院自动化系

Content

- **Introduction**
- **A Cross Application Research to Block Cipher and Artificial Intelligence**
- Intelligent Applications of Block Cipher in Different Network Layers
- **PostPHD direction : Some Applications of the Cross Research**
- Philosophy: Bayesian Model & Cryptography
- Lightweight Block Ciphers and the Cross Research (RFID、DRM)
- Quantum and the Cross Research
- **Appendices**

目 录

- 简介
- 分组密码和人工智能交叉应用研究
- 分组密码在不同开放网络层上的应用
- 一些交叉应用研究（博后研究方向）
- 原理: 贝叶斯模型和分组密码
- 轻型分组密码和交叉应用研究 (DRM, RFID)
- 量子和交叉应用研究
- 附录

Abstract

- The cross application research of block cipher and artificial intelligence becomes an important direction because of the cognition to Internet, RFID, DRM, quantum communication. The intelligent application in trust network can be merged with Internet and implement in different layers. Furthermore, the intelligent application with block ciphers and kinds of networks is a large scale research direction. With the same design principal of stream cipher, block cipher and HASH, the memory module design with the block cipher must use the Artificial Intelligence idea. The sound automation with the memory module is the simple result of multi-layers application.

简 介

随着开放网络、RFID、DRM、量子通信、可信网络的的认知和应用，分组密码和人工智能交叉应用研究成为一个前端的方向。就分组密码本身设计而言，随着流密码、分组密码、HASH的融合趋势，带记忆的分组密码设计本身就含有人工智能元素，如果对记忆程度进行最优的智能处理，可以简单的满足跨网络层次使用。

TSINGHUA UNIVERSITY

Cross Application Research to Block Cipher and Artificial Intelligence

- **Intelligent Applications of Block Cipher in Different Network Layers**

- Introduction
- Cross Application Research
- Different Block Ciphers & Different Modes (TCP/IP)
- Main Results

Intelligent Applications of Block Cipher in Different Network Layers (1)

- **Introduction**

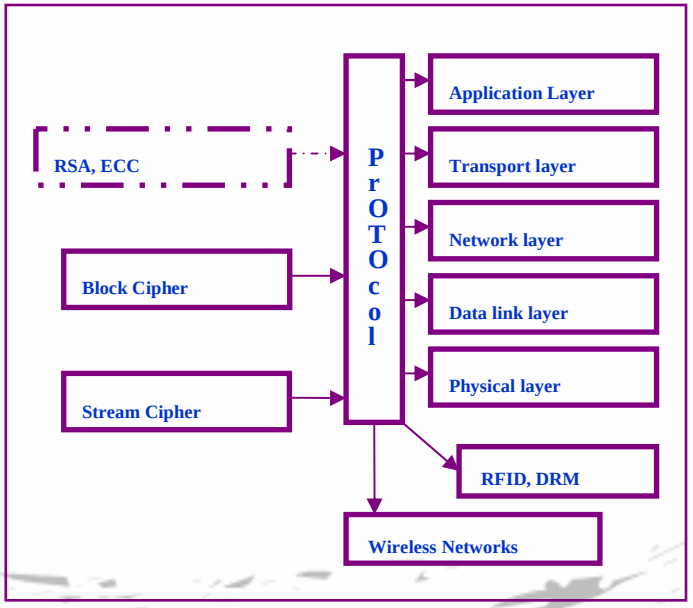
- A block cipher is a type of cryptographic system that usually strengthen internet network and wireless networks more security. It is one of most active directions in published field of cipher algorithm and symmetric key encryption. The weights of symmetric ciphers based on Bayesian model are the necessary studies because of quality of services.

Intelligent Applications of Block Cipher in Different Network Layers (2)

- **Cross Application Research**
- **Precise weight of symmetric cipher based on Bayesian model**
- **Bayesian model of symmetric cipher**
- Bayesian inference is a rational engine for solving such problems within a probabilistic framework, and consequently is the heart of most probabilistic models of weighing the ciphers. Causal Bayesian networks are identified with theories at the lowest, most concrete level of the abstraction hierarchy, level T0. We define the security of cipher as T2, T1 is the cipher itself and D is the networks environment. In Bayesian model, we can judge the cipher's weight according to value of *P* directly.

Intelligent Applications of Block Cipher in Different Network Layers (3)

- **Cross Application Research**
- **Precise weight in Bayesian model**
- Symmetric ciphers make optimal inferences from others' behavior given knowledge of this relation-ship The relationship between preferences and choices has been the subject of extensive research in economics and psychology.



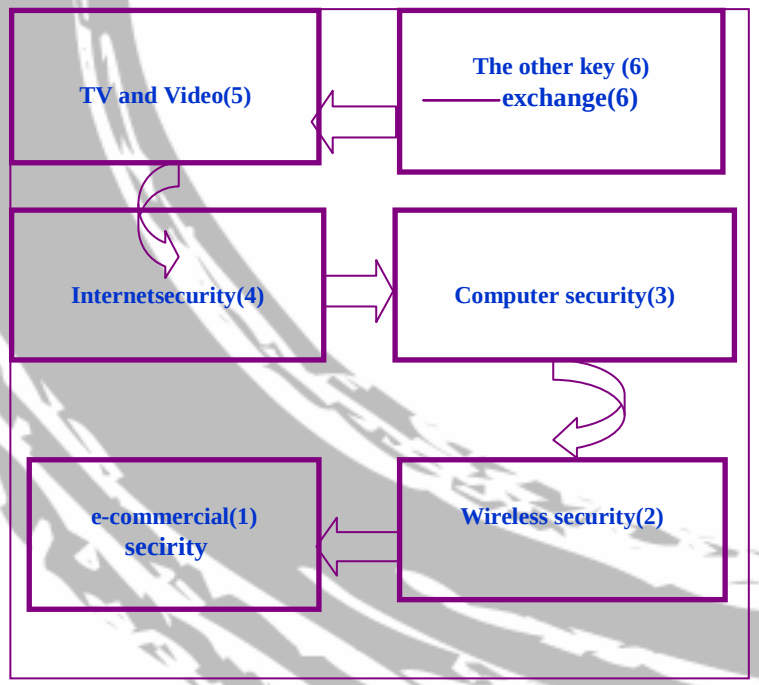
Intelligent Applications of Block Cipher in Different Network Layers (4)

- **Cross Application Research**
- **The ciphers' precise weight according to Bayesian model**

- The stream ciphers are often utilized at network layer, link layer and other kinds of networks, such as RFID, DRM, wireless networks. The block ciphers are utilized at transport layer, application layers and other networks. Because of the stream cipher mode, the block ciphers can use as stream ciphers and suit for the environment of stream ciphers. The number of stream ciphers is more than that of block cipher. Because the weight of stream cipher is lighter than block cipher, the stream ciphers are often used at lower layers of TCP/IP, such as Network layer, Link layers. Furthermore, the precise categorization of stream cipher should be researched.

- **The weight of block ciphers is heavier than that of the stream ciphers.**

Intelligent Applications of Block Cipher in Different Network Layers (5)



- **Cross Application Research**
- **The protocols' precise weight according to Bayesian model**

- The Internet security protocols are categorized by the different layers, which are lighter in top layers than in lower layers. Meanwhile, in computer security, the hardware protocols are heavier than OS protocol. The wireless protocols are weakness and the e-commercial can be considered as the special application layer of internet. When e-commercial is focused on e-bank, its weight is even heavier than wireless security.

Intelligent Applications of Block Cipher in Different Network Layers (6)

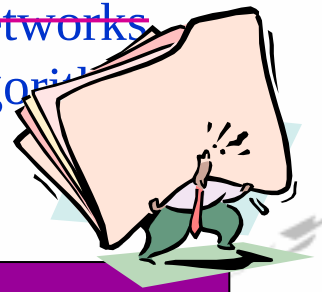
- **Main Results**
- **Intelligent application of symmetric ciphers is a direction that uses Bayesian model of cognition science. Because of the stream ciphers are utilized at lower layer meanwhile the block ciphers are utilized at toper layer of TCP/IP. Furthermore, we also study the intelligent conversion of the symmetric ciphers. There are some protocols go with the application of those weighted cipher on different networks by optimal choice.**

Related Papers

- Lan Luo, ZhiGuang Qin, Juan Wang, The Intelligent Conversion for Different Layers‘ Block Ciphers, ICIC Express Letters, Volume 3, Issue 1, March 2009, pp.73–77.（SCIE，EI）
- Lan Luo, ZhiGuang Qin, ShiJie Zhou, A Comment to the Intelligent Functions of Different Weight Ciphers, IEEE proceeding of WKDD2009.（EI）

PostPHD Direction:
Some Applications of the Cross Research

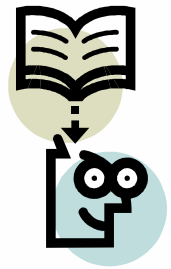
- ~~Philosophy: Bayesian Models & Cryptography~~ (finished)
- ~~Lightweight Block Ciphers and the Cross Research~~ (finished)
- ~~Quantum and the Cross Research~~ (finished)
- ~~Trusted Network and the Cross Research~~ (finished)
- ~~Transformation of Block Ciphers in Different Networks~~
- (finished, maybe I will publish a block cipher algori



THE NETWORKS AS THE PLATFORM

Philosophy: Cryptography & Bayesian Model

- The Symmetric Ciphers and Protocols Weigh in Bayesian Model
- The Ciphers Weigh in Faithful Transmission



Related Papers

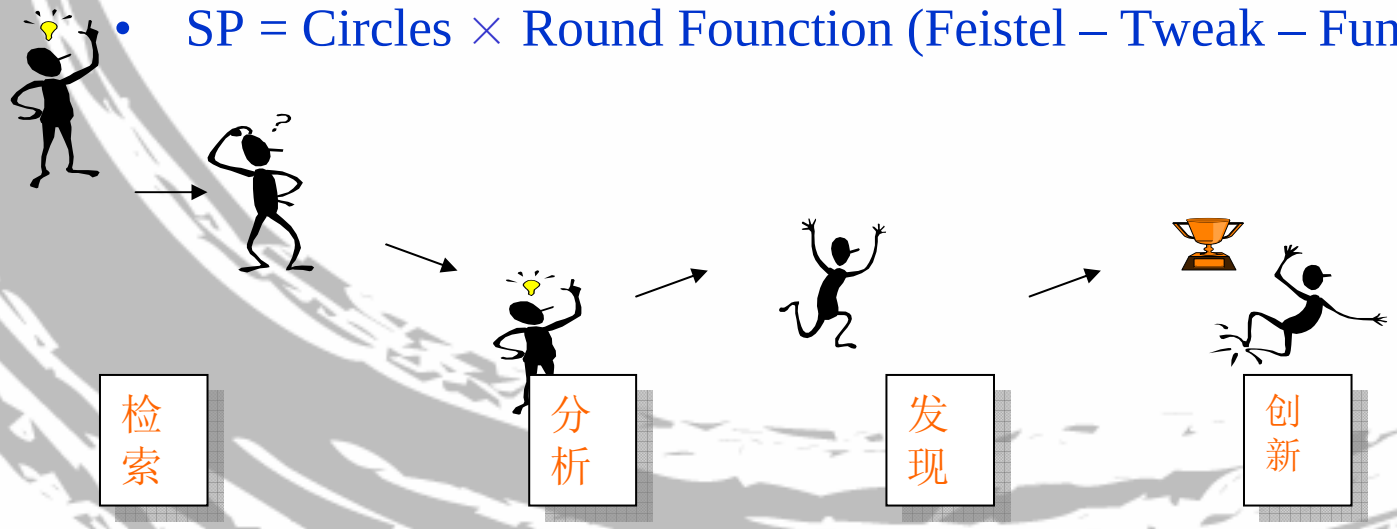
- Lan Luo, Rong Fang, XiangYang Ji, GuoGen Wan, A Study to the Symmetric Ciphers and Protocols Weigh in Bayesian Model IJCC, Sept 2010
- Lan Luo, QiongHai Dai, Rong Fang, A Study to the Ciphers Weigh in Faithful Transmission （submitted）

Transformation of Block Ciphers in 2 Structures

- The block cipher's two round structures are initially transformed when they fuse into LFSR. SP structure can be considered two F functions in one Feistel round function which combines both right and left of origin data transformation. Furthermore, the round number linear function and nonlinear function of Feistel and SP structure are compared. The merit of SP structure is that it can fuse in LFSR as a nonlinear filter without memory.

Related Paper

- Lan Luo, ZeHui Qu, ChaoMing Song, Precise Transformation of Feistel to SP Fuse into LFSR （SCIE）
- Feistel = SP + Memory + Twist
- SP = Circles × Round Founction (Feistel – Tweak – Function)



Appendices

- A Note to the Block Cipher as Stream Cipher
- Golden Fish: An Intelligent Stream Cipher Fuse Memory Modules
- A Middleware Design for Block Cipher Seamless Connected into Stream Cipher Mode
- The Intelligent Secure Structure Based on Active Block Cipher for Application Layer of Network

A Note to the Mode of Block Cipher as Stream Cipher

- A block cipher is used as nonlinear function is a kind of economic method to promote the security. OFB mode made block cipher operating as a stream cipher and CFB mode take as the cipher self-synchronization encipher mechanism.
- There is CTR mode that also can convey block cipher to stream cipher. But the character of string generated by such kind of mode is even not controlled by designers themselves.

TSINGHUA UNIVERSITY

A Middleware Design for Block Cipher Seamless Connected into Stream Cipher Mode

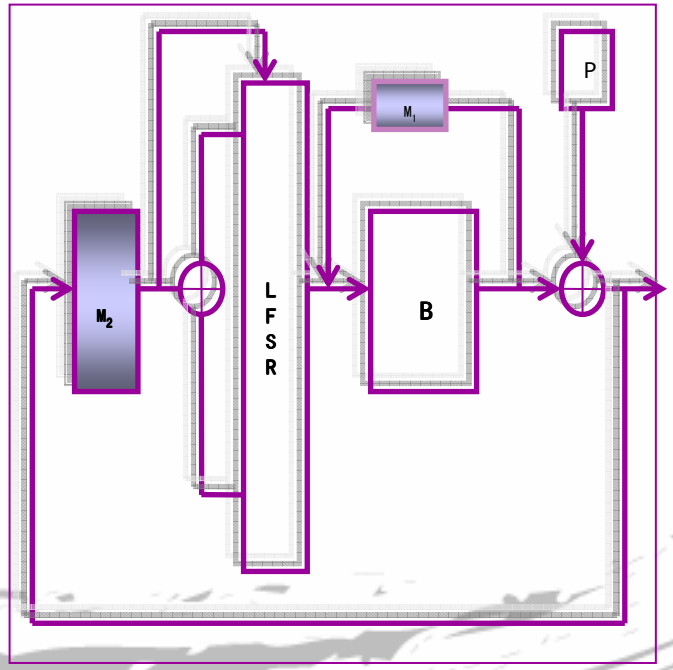
- The block cipher is used as nonlinear function is a kind of economic method to promote the security. The middleware part is a simple way to solve the seamless connect the block cipher operate as a stream cipher. Sometimes, such flexibility and scalable model can be named cryptography middleware.

The Intelligent Secure Structure Based on Active Block Cipher for Application Layer of Network

- We choose kinds of block cipher algorithms as the active database for intelligent choice on both access authentication and data confidential. The intelligent secure mechanism actually is an overlay upon the TCP/IP the same as P2P structure. Because of the intelligent choice the effect and security level are optimized.
- 4 block ciphers are transformed to
- **N= (3×3×3+3×3×2+3×3×3+3×3×1)×8**
- = **648** block ciphers

Golden Fish: An Intelligent Stream Cipher Fuse Memory Modules

- Such kind of design (Mi) can be found at Shabal, Luffa & Keccak of SHA3
- Indeed, security trades off the efficiency for current algorithm. Practically, the block cipher is applied as nonlinear function, as an economic method to promote the security. Furthermore, the realization of modules Mi, Module B and LFSR is highly flexible and transformable.



•ePrint.iacr.org/2009/611

Related Papers

- Lan Luo, ZhiGuang Qin, ShiJie Zhou, A Middleware Design for Block Cipher Seamless Connected into Stream Cipher Mode, IEEE proceeding of IIH-MSP2008（EI）
- Lan Luo, ZhiGuang Qin, ShiJie Zhou, The Intelligent Secure Structure Based on Active Block Ciphers for Application Layer of Internet , IEEE proceeding of CISP2008 （EI）
- Lan Luo, ZhiGuang Qin, Shaoquan Jiang, A Key Delay Design Operation Model of Block Cipher Algorithm in Networks, proceeding of ISKE2007（ISTP）

Thank you for your attention