特定非営利活動法人 日中科学技術交流協会

2012年度中国人留学生研究奨励賞研究発表

2012年12月21日　東京大学本郷山上会館

① 李　陽（LI, Yang）(江蘇省鎮江市、1986.4.26生れ)
電気通信大学大学院 情報理工学研究科 総合情報学専攻 博士課程2年
研究テーマ：故障利用物理攻撃とその対策
指導教員：准教授　崎山一男

② 元　金石（YUAN, Jinshi）(黒龍江省ハルビン市、1983.4.13生れ)
筑波大学/物質・材料研究機構　連携大学院　博士課程修了(2012.7博士号取得)
物質・材料研究機構　1次元材料グループ　ポスドク研究員(2012. 8から)
研究テーマ：ハフニウム炭化物単結晶ナノワイヤの作成と電子源 への応用
指導教員：筑波大学 数理物質科学研究科　准教授　唐　捷

③ 張　治宇（ZHANG, Zhiyu）(四川省重慶市、1985. 5.20生れ)
九州大学/物質・材料研究機構　連携大学院　博士課程3年
研究テーマ：強磁場発生用超伝導磁気レンズの開発
指導教員：教授　木吉　司

1

李くんの研究紹介

電気通信大学
崎山一男
Dec. 21st,2012

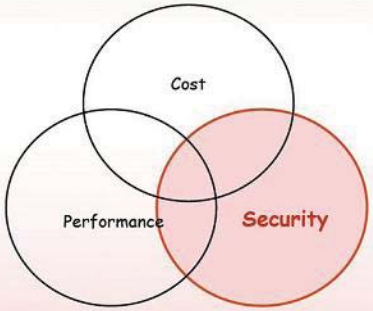
情報セキュリティシステム

- 日常におけるセキュリティシステム
  - 携帯電話，RFIDタグ，スマートカード，バイオメトリクス，etc.

2

暗号実装の3大要素

- 低コスト・高性能に加えて
  - コスト－性能－セキュリティ（安全性）のトレードオフ



3

耐タンパー性の向上

- 暗号実装における安全性
  - 数学的に安全な暗号 ≠ 暗号を実装したシステムが安全
  - 情報漏えいはシステムの最も脆弱な部分から
  - 暗号実装（デバイス）からの情報漏れを防ぐ

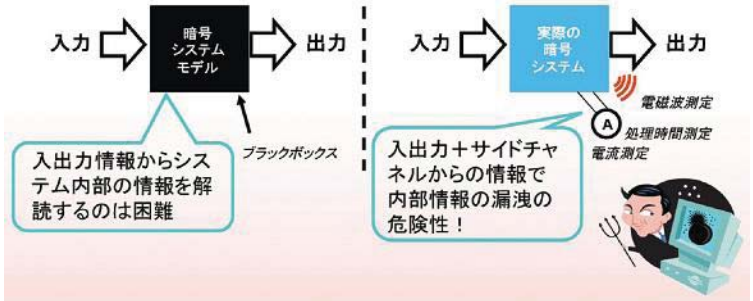
A chain is as strong as it weakest link

セキュリティシステムと暗号実装

- システム要求と暗号実装での仕様
- 暗号デバイスの性能とシステム性能
- 暗号理論と暗号実装

暗号実装に対する脅威

- サイドチャネルとは？
  - 暗号実装システム (主にLSI) に対して



攻撃の分類

- 暗号実装への攻撃

New Fault-Based Physical Attacks And Their Countermeasures
新たな故障利用物理攻撃とその対策に関する研究

太田・崎山研究室
Yang Li (李陽)
Dec. 21nd,2012

自己紹介

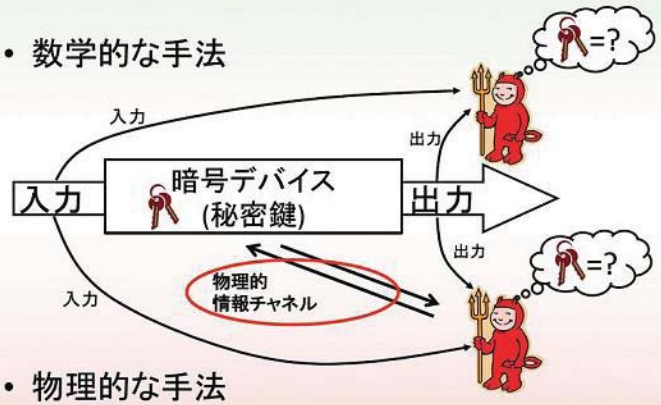
- 李阳（李陽），Yang Li
- 1986年6月　生まれ
- 出身地：中国江蘇省鎮江市（上海に近い）
- 電気通信大学大学院
  - 情報理工学研究科 総合情報学専攻
  - 博士課程 2 年 （本日学位授与）
- 指導教員：崎山一男 准教授

目　次

暗号デバイスはどこにでもある

暗号解析攻撃

- 数学的な手法



- 物理的な手法

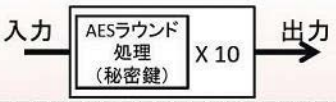
12

物理攻撃

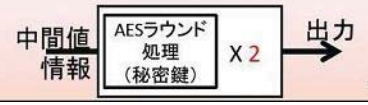
- 現実的な脅威(例えば　Mifare DESFire MF3ICD40)
- 非常に強力な攻撃
  - 中間値情報のアクセス
  - 部分的なアルゴリズムを攻撃

Advanced Encryption Standard(AES)128ビット　バージョン

数学的な手法:
AES-128(10ラウンド)
鍵復元が困難



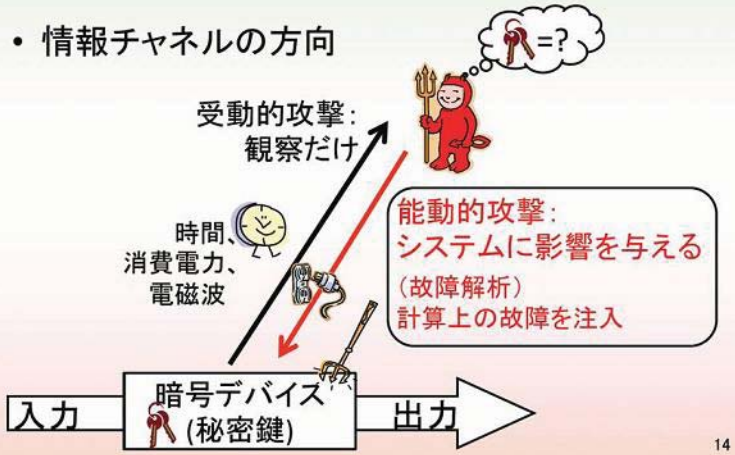
物理的な手法:
部分的なAES-128(2ラウンド)
鍵復元が簡単



13

物理的な攻撃の分類(1)

- 情報チャネルの方向



14

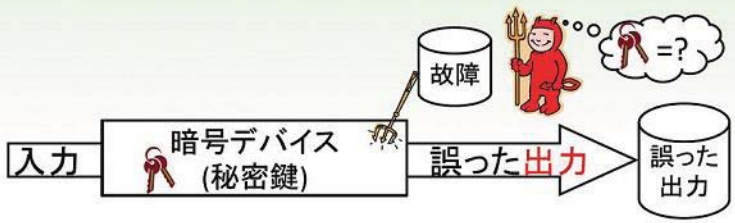
物理攻撃の分類(2)

- チップへの侵入度

	侵入型	半侵入型	非侵入型
パッケージを破る	必要	必要	不要
電子的なやり取り	必要	不要	不要
デバイスを壊す	必要	必要	不要
攻撃費用			

15

非侵入型 故障注入方法



非侵入的な故障:

正確な
タイミング

不規則なクロック: 24MHz→70MHz

不規則な給電: 3.3V→1.8V

不規則な温度: 25℃→120℃

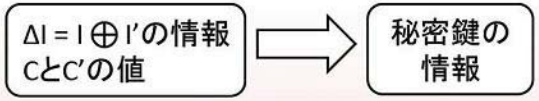
非侵入型故障注入の現実性

- リソース制限付きデバイス
  - スマートカード(Suicaカード)
- 本研究の実験:サイドチャネル攻撃標準評価ボード(SASEBO-R)

AES暗号への差分故障解析(DFA)

- 差分故障解析(DFA)

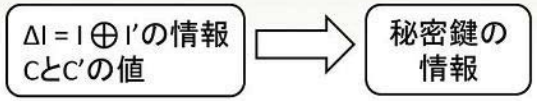
- DFAの鍵復元



- DFAの対策
  - 誤った出力C'の値を隠す

差分故障解析(DFA)とその対策

- 差分故障解析



- 対策: C'の値を隠す
  - ゲート·レベルの実現:
    - Wave Dynamic Differential Logic (WDDL)
  - アルゴリズム·レベルの実現:
    - AES-with–Error-Detection

C'値を隠す方法

- WDDL
  - 故障が注入されると、変な演算が行われる

普通の回路:	WDDL回路
1 → 0	1 → "Null"
0 → 1	0 → "Null"

- AES-with–Error-Detection
  - 故障を検出すると、C'を出力しない

主なアイデア： 故障注入強度の導入

- 先行研究における故障注入

正常の実行	故障注入の実行
24MHz	70MHz
3.3V	1.8V
25℃	120℃

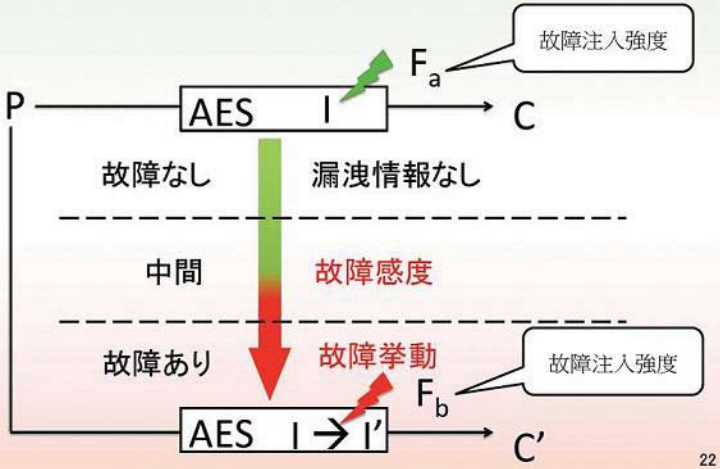
DFAのためには、最適な故障を注入するパラメータを見つける

- 本研究においての故障注入

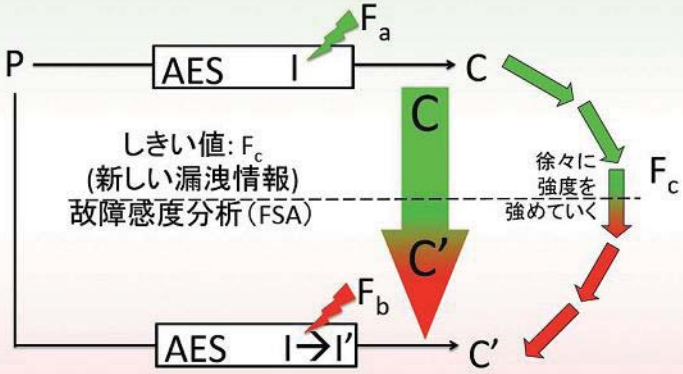
正常の実行	故障注入の実行
24MHz	70MHz
3.3V	1.8V
25℃	120℃

"故障注入強度" ⇨ "新しい攻撃＆新たな対策"

新しい故障ベースの情報漏洩



故障感度とは

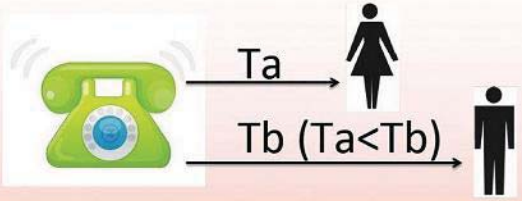


FSは中間値Iの値に依存するから，鍵復元に使える.

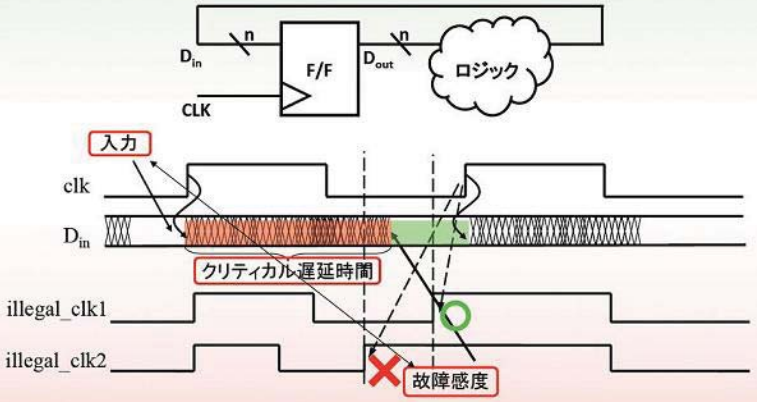
故障感度分析はC'の値を知らなくていい.

実際の生活での例

- 家に電話をかけるときに、声を聞かずに、私は誰が（母あるいは父）電話に応答するかを知ることができる
- 母が電話に応答するまでの時間は父より短い
- 母は電話に父より敏感である

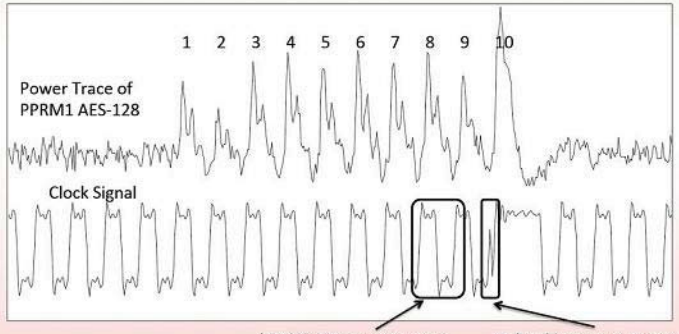


不正なクロック下での故障感度

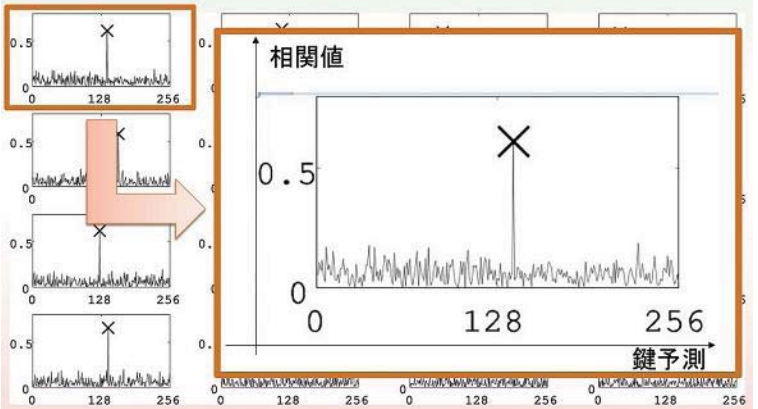


不正クロックの例

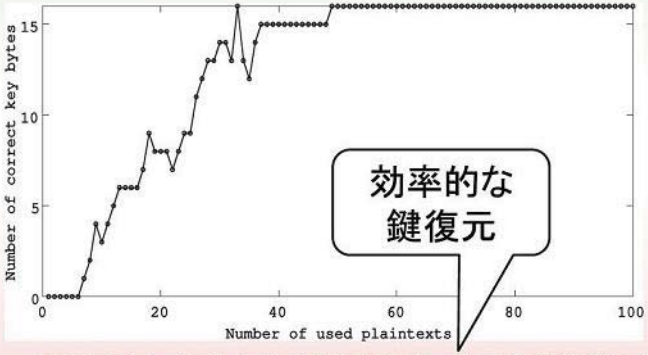
- 消費電力波形とクロック信号



故障感度解析の鍵復元例（PPRM1-AES）



必要なデータ量



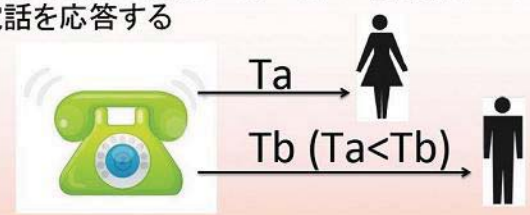
50個の平文に対応する故障感度データで全鍵を復元

故障感度解析の意義

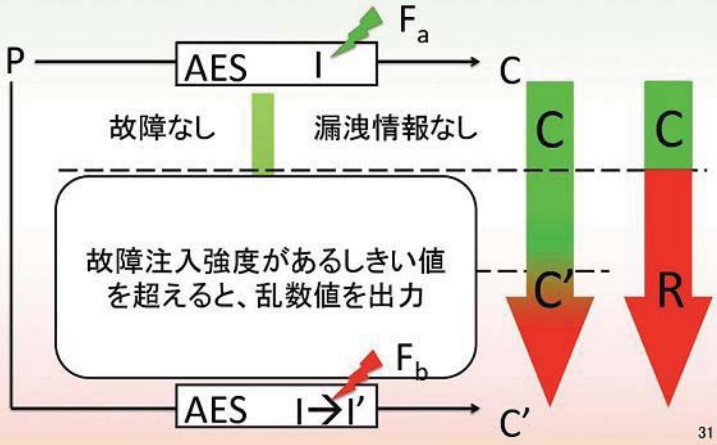
- これまでの対策を破る: C'値を隠す
  - ゲート·レベル: WDDL
    - 故障が注入されると、変な演算が行われる
  - アルゴリズム·レベル: AES-with–Error-Detection
    - 故障を検出すると、C'を出力しない
  - Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "New Fault-Based Side-Channel Attack using Fault Sensitivity," IEEE Trans. Inf. Forensic Secur., Vol.7, No. 1, pp. 88-97, (Feb., 2012).
- 故障注入が区別できる限り、故障感度解析は適用可能です。

故障感度解析の対策

- 家に電話をかけるときに、声を聞かずに、私は誰が(母あるいは父)電話に応答するかを知ることができる
- 母が電話に応答するまでの時間は父より短い
- 母は電話に父より敏感である
- 対策:両親が約束して、一定の時間を待ってから、電話を応答する



故障ベースの情報漏えいを隠すには



まとめ

- “故障注入強度”という概念を導入することによって、本研究は故障ベースの漏洩を拡張し、新たな攻撃を提案した
- 拡張した漏洩情報を考慮して、故障感度と誤った出力の両方を隠すことで対策を提案した

ご清聴ありがとうございました

Related Publications (1)

- Journal Papers (3)
  - 1. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, “A New Type of Fault-Based Attack: Faulty Behavior Analysis” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., to appear. Related to Chap. 5
  - 2. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, “New Fault-Based Side-Channel Attack using Fault Sensitivity,” IEEE Trans. Inf. Forensic Secur., Vol.7, No.1, pp.88-97, (Feb., 2012). Related to Chap. 4
  - 3. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, “Toward Effective Countermeasures Against An Improved Fault Sensitivity analysis,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A95-A, No. 1, pp.234-241, (Jan., 2012). Related to Chap. 8
- Refereed Conference Papers (with Formal Proceedings) (1)
  - 1. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, “Revisit Fault Sensitivity Analysis on WDDL-AES,” In Proc. International Symposium on Hardware-Oriented Security and Trust (HOST’11), IEEE, pp.148-153, (Jun., 2011). Related to Chap. 5

Related Publications (2)

- Referred Presentations (2)
  - 1. 李陽, 太田和夫, 崎山一男, “Sensitive-Data Dependency of Faulty Behavior and Its Application,” 2012年 暗号と情報セキュリティシンポジウム (SCIS2012), 3C1-3E, 7 pages, (Feb., 2012)} *Related to Chap. 6*
  - 2. Yang Li, Kazuo Ohta, Kazuo Sakiyama“[Invited talk] Break Masked AES Implementations Using Fault Sensitivity and Faulty Ciphertext: Review of Presentation at CHES2011.” 情報セキュリティ研究会（ISEC）2011, (Dec. 14nd, 2011). *Related to Chap. 6*

All publications (1/4)

- **Book Chapters (1)**
  - Junko Takahashi, Toshinori Fukunaga, Shigeto Gomisawa, **Yang Li**, Kazuo Sakiyama, and Kazuo Ohta, "Fault Injection and Key Retrieval Expariments on Evaluation Board," Chapter in Marc Joye and Michael Tunstall editors, Fault Analysis in Cryptography, Springer, (to appear in Jun., 2012).
- **Journal Papers (6)**
  - **Yang Li**, Kazuo Ohta, and Kazuo Sakiyama, "A New Type of Fault-Based Attack: Faulty Behavior Analysis" IEICE Trans. Fundam. Electron. Commun. Comput. Sci., to appear
  - 小池彩歌,**李陽**,中津大介,太田和夫,崎山一男,"複数の要因に対する新たな故障感度解析,"電子情報通信学会論文誌(A), Vol. J95, No.10, pp. 751-755, (Oct. 2012)
  - Kazuo Sakiyama, **Yang Li**, Mitsugu Iwamoto, and Kazuo Ohta, "Information-Theoretic Approach to Optimal Differential Fault Analysis," IEEE Trans. Inf. Forensic Secur., Vol.7, No.1, pp.109-120, (Feb., 2012).
  - **Yang Li**, Kazuo Ohta, and Kazuo Sakiyama, "New Fault-Based Side-Channel Attack using Fault Sensitivity," IEEE Trans. Inf. Forensic Secur., Vol.7, No.1, pp.88-97, (Feb., 2012).
  - **Yang Li**, Kazuo Ohta, and Kazuo Sakiyama, "Toward Effective Countermeasures Against An Improved Fault Sensitivity Analysis," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A95-A, No.1, pp.234-241, (Jan., 2012).
  - **Yang Li**, Kazuo Sakiyama, Shinichi Kawamura, and Kazuo Ohta, "Power Analysis against a DPA-resistant S-box Implementation Based on the Fourier Transform," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A94-A, No.1, pp.191-199, (Jan., 2011).

All publications (2/4)

- **Refereed Conference Papers (with Formal Proceedings) (12)**
  - Nakasone Toshiki, **Yang Li**, Yu Sasaki, Mitsugu Iwamoto, Kazuo Ohta and Kazuo Sakiyama, "Key-Dependent Weakness of AES-Based Ciphers Under Clockwise Collision Distinguisher," In Proc. the 15th Annual International Conference on Information Security and Cryptology (ICISC'12), LNCS, (to appear).
  - **Yang Li**, Kazuo Ohta and Kazuo Sakiyama, "An Extension of Fault Sensitivity Analysis Based on Clockwise Collision," In Proc. the 8th China International Conference on Information Security and Cryptology (Inscrypt'12), LNCS, (to appear).
  - Sho Endo, **Yang Li**, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta and Takafumi Aoki,"An Efficient Countermeasure against Fault Sensitivity Analysis Using Configurable Delay Blocks," In Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC'12), IEEE, (Sep., 2012).
  - Yu-ichi Hayashi, Shigeto Gomisawa, **Yang Li**, Naofumi Homma, Kazuo Sakiyama, Takafumi Aoki, and Kazuo Ohta, "Intentional Electromagnetic Interference for Fault Analysis on AES Block Cipher IC," In Proc. International Workshop on Electromagnetic Compatibility of Integrated Circuits (EMCCOMPO'11), IEEE, pp.235-240, (Nov., 2011).
  - Amir Moradi, Oliver Mischke, Christof Paar, **Yang Li**, Kazuo Ohta, Kazuo Sakiyama, "On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attack in a Combined Setting," In Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES'11), LNCS 6917, Springer-Verlag, pp.292-311, (Sep., 2011).
  - Hikaru Sakamoto, **Yang Li**, Kazuo Ohta, and Kazuo Sakiyama, "Fault Sensitivity Analysis Against Elliptic Curve Cryptosystems," In Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC'11), IEEE, pp.11-20, (Sep., 2011).
  - **Yang Li**, Kazuo Ohta, and Kazuo Sakiyama, "Revisit Fault Sensitivity Analysis on WDDL-AES," In Proc. International Symposium on Hardware-Oriented Security and Trust (HOST'11), IEEE, pp.148-153, (Jun., 2011).
  - Yu Sasaki, **Yang Li**, Lei Wang, Kazuo Sakiyama, and Kazuo Ohta, "New Approach of Super-Sbox Analysis on AES-Based Permutations: Applications to ECHO and Grostl," In Proc. Advances in Cryptology ASIACRYPT'10, LNCS 6477, Springer-Verlag, pp.38-55, (Dec., 2010).
  - Daisuke Nakatsu, **Yang Li**, Kazuo Sakiyama, and Kazuo Ohta, "Combination of SW Countermeasure and CPU Modification on FPGA Against Power Analysis," In Proc. International Workshop on Information Security Applications (WISA'10), LNCS 6513, Springer-Verlag, pp.258-272, (Aug., 2010).
  - **Yang Li**, Kazuo Sakiyama, Shigeto Gomisawa, Toshinori Fukunaga, Junko Takahashi, and Kazuo Ohta, "Fault Sensitive Analysis," In Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES'10), LNCS 6225, Springer-Verlag, pp.320-334, (Aug., 2010).
  - **Yang Li**, Kazuo Sakiyama, Lejla Batina, Daisuke Nakatsu, and Kazuo Ohta, "Power Variance Analysis Breaks a Masked ASIC Implementations of AES," In Proc. Design, Automation and Test in Europe (DATE'10), ACM, pp.1059-1064, (Mar., 2010).
  - **Yang Li**, Kazuo Sakiyama, Shinichi Kawamura, Yuichi Komano, and Kazuo Ohta, "Security Evaluation of a DPA-resistant S-box Based on the Fourier Transform," In Proc. International Conference on Information and Communications Security (ICICS'09), LNCS 5927, Springer-Verlag, pp.3-16, (Dec., 2009).

All publications (3/4)

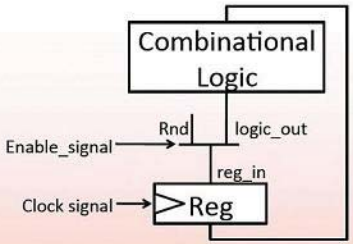
- **Non-refereed Papers (24)**
  - 李陽, 太田和夫, 崎山一男, "Sensitive-Data Dependency of Faulty Behavior and Its Application," 2012年 暗号と情報セキュリティシンポジウム (SCIS2012), 3C1-3E, 7 pages, (Feb., 2012)
  - 中曽根俊貴, 中津大介, **李陽**, 太田和夫, 崎山一男, "クロック間衝突を利用した電磁波解析," 2012年 暗号と情報セキュリティシンポジウム (SCIS2012), 3C1-1, 8 pages, (Feb., 2012)
  - 小池彩歌, **李陽**, 中津大介, 太田和夫, 崎山一男, "IRドロップを利用した故障感度解析と高温環境下における影響," 2012年 暗号と情報セキュリティシンポジウム (SCIS2012), 2C3-3, 7 pages, (Jan., 2012)
  - 中津大介, **李陽**, 太田和夫, 崎山一男, "テンプレートを利用した時系列電力解析," 2012年 暗号と情報セキュリティシンポジウム (SCIS2012), 2C2-5, 6 pages, (Jan., 2012)
  - **Yang Li**, Kazuo Ohta, Kazuo Sakiyama"[Invited talk] Break Masked AES Implementations Using Fault Sensitivity and Faulty Ciphertext –Review of Presentation at CHES2011–" 情報セキュリティ研究会（ISEC）2011, (Dec. 14nd, 2011).
  - 阪本光, **李陽**, 太田和夫, 崎山一男, "クロック間衝突を用いた楕円曲線暗号実装に対する故障感度解析," ISEC2011-49, pp.101-108, (Nov., 2011).
  - Toshiki Nakasone, Daisuke Nakatsu, **Yang Li**, Kazuo Ohta, Kazuo Sakiyama, "First Experimental Results of Correlation-Enhanced EMA Collision Attack," Poster Session, CHES2011 (Sept., 2011).
  - **Yang Li**, Daisuke Nakatsu, Qi Li, Kazuo Ohta, Kazuo Sakiyama, "Clockwise Collision Analysis — Overlooked Side-Channel Leakage Inside Your Measurements–," Cryptology ePrint Archive, Report 2011/579, 2011.
  - 高柳真如, 佐々木悠, **李陽**, 太田和夫, 崎山一男, "7及び8ラウンド既知鍵AES識別機の実装," 2011年 暗号と情報セキュリティシンポジウム (SCIS2011), 2B2-4, 7 pages, (Jan., 2011).
  - **李陽**, 太田和夫, 崎山一男, "Self-Template Fault Sensitivity Analysis," 2011年 暗号と情報セキュリティシンポジウム (SCIS2011), 3D3-1, 8 pages, (Jan., 2011).
  - 阪本光, **李陽**, 太田和夫, 崎山一男, "楕円曲線暗号実装に対するFault Sensitivity Analysis," 2011年 暗号と情報セキュリティシンポジウム (SCIS2011), 3D3-2, 8 pages, (Jan., 2011).
  - Shigeto Gomisawa, **Yang Li**, Junko Takahashi, Toshinori Fukunaga, Yu Sasaki, Kazuo Sakiyama, Kazuo Ohta, "Efficient Differential Fault Analysis for AES," Cryptology ePrint Archive, Report 2010/336, 2010.

All publications (4/4)

- **Non-refereed Papers (24)**
  - **Yang Li**, Shigeto Gomisawa, Kazuo Sakiyama, and Kazuo Ohta, "An Information Theoretic Perspective on the Differential Fault Analysis against AES," Cryptology ePrint Archive, Report 2010/032, 2010.
  - Naoyuki Takayanagi, **Yang Li**, Kazuo Sakiyama, and Kazuo Ohta, "Effective Verification for Known-Key Distinguisher by Using Extended Differential Path," In Proc. Triangle Symposium on Advanced ICT 2010 (TriSAI'10), pp.284-287, (Oct., 2010).
  - 岩本貢, **李陽**, 崎山一男, 太田和夫, "回転操作が可能な視覚復号型秘密分散法の一般的構成法," ISEC2010-49, pp.67-74, (Sept., 2010).
  - Yu Sasaki, **Yang Li**, Lei Wang, Kazuo Sakiyama, and Kazuo Ohta, "New Non-Ideal Properties of AES-Based Permutations: Applications to ECHO and Grostl," The Second SHA-3 Candidate Conference, (Aug., 2010).
  - 五味澤重友, 泉雅巳, **李陽**, 高橋順子, 福永利徳, 佐々木悠, 崎山 一男, 太田和夫, "AES暗号実装へのフォールト解析攻撃における適用範囲の拡大と解析効率の向上 ," 2010年 暗号と情報セキュリティシンポジウム (SCIS'10), 2B1-1, 6 pages, (Jan., 2010).
  - **Yang Li**, Shigeto Gomisawa, Kazuo Sakiyama, and Kazuo Ohta, "An Information Theoretic Perspective on the Differential Fault Analysis against AES," 2010 Symposium on Cryptography and Information Security (SCIS'10), 2B1-2, 6 pages, (Jan., 2010).
  - 中津大介, **李陽**, 崎山一男, 太田和夫, "DPA耐性のあるソフトウェア実装のための安全なCPU," 2010年 暗号と情報セキュリティシンポジウム (SCIS'10), 2B3-1, 6 pages, (Jan., 2010).
  - **Yang Li**, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama, "Visual Secret Sharing Schemes Allowing Arbitrary Rotation Angles of Shares," In Proc. Triangle Symposium on Advanced ICT 2009 (TriSAI'09), Tokyo, Japan, pp.33-38, (Oct., 2009).
  - Daisuke Nakatsu, **Yang Li**, Kazuo Sakiyama, and Kazuo Ohta, "Comparison of Masked S-boxes in Hardware Implementation," In Proc. Triangle Symposium on Advanced ICT 2009 (TriSAI'09), Tokyo, Japan, pp.176-181, (Oct., 2009).
  - **Yang Li**, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama, "A Novel Construction Method for Visual Secret Sharing Schemes Allowing Rotation of Shares," ISEC2009-5, pp.29-36, (May, 2009).
  - **Yang Li**, Mengyu Zhu, Wang Lei, Kazuo Ohta, and Kazuo Sakiyama, "Visual Secret Sharing Schemes for Multiple Secret Images Allowing the 90-degree Rotation of Shares," 2009 Symposium on Cryptography and Information Security (SCIS'09), 1F1-3, (Jan., 2009).
  - Bagus Santoso, **Yang Li**, Kazuo Ohta, "Generalizing Micropayment system based on Probabilistic Polling," 2008 Symposium on Cryptography and Information Security (SCIS'08), 3E4-5, (Jan., 2008).

Conceal fault-based leakage

- Use *enable signal* to conceal Fault Sensitivity
  - Enable is 1 only when fault intensity is in fault-free zone
- Use *random value* to conceal Faulty Output



If Enable==0
  Register ← Random Value
If Enable==1
  Register ← Calculation Result

Discussion about proposed CM

- How to realize the enable signal?
  - S. Endo, Y. Li, N. Homma, K. Sakiyama, K. Ohta, and T. Aoki. "An Efficient Countermeasure Against Fault Sensitivity Analysis Using Configurable Delay Blocks." In FDTC 2012
  - About 10.4% area overhead
- How about other fault injections
  - Laser, invasive fault injections?