

コンテンツ配信管理システムとその安全性確認に関する研究 (研究課題番号：16016258)

研究代表者 藤原 融 大阪大学・大学院情報科学研究科
研究分担者 石原 靖哲 大阪大学・大学院情報科学研究科
吉田 真紀 大阪大学・大学院情報科学研究科

1 研究の概要

情報通信技術の進歩に伴い、より大規模でかつ複雑な論理的構造をもつコンテンツの配信がますます盛んになると考えられる。本研究では、論理的構造をもつコンテンツの配信管理も含め、コンテンツ配信管理システムやそれに関わる様々なセキュリティの問題の解決を行ってきた。行った研究は、コンテンツ配信管理システムの開発に関する研究、コンテンツ配信管理の安全性に関する研究、コンテンツ配信管理に役立つ要素技術の研究の3つに大別できる。

コンテンツ配信管理システムの開発に関する研究では、システムとして放送型や委託配信型、コンテンツとして構造のないものやインタラクティブドラマなどの分岐構造をもつものについて、配信管理システムの設計を行った。また、構造をもつコンテンツのアクセス権限の管理法として、アクセス制御ポリシーが規定されたXML文書におけるビュー（すなわち、そのポリシーによって読み出しを許可されたすべての部分文書）を切り出すプログラム（ビュー定義）を自動生成するツールの開発も行った。安全性に関する研究としては、より一般の暗号プロトコルやデータベースも視野に入れ、オブジェクト指向データベースにおける推論攻撃に対する安全性、安全でない暗号プロトコルに対する攻撃法導出に関する研究も行った。さらに、要素技術の研究としては、分離不能多重化通信、時間限定サービス、XML文書の統合などの研究を行った。以下、各年度の研究内容の概要を示す。

初年度（平成13年度）は、コンテンツの構造のモデル化に関して検討し、有向グラフからXMLデータまでの様々なレベルのいくつかの抽象度で考えることとした。そして、有向グラフのような抽象度を対象とし動的に構造が変化する場合も含め構造に即した取得権限の管理法（暗号化鍵の管理法）の検討を行った。その他にも、コンテンツ配信管理の安全性として、データベースに対する推論攻撃の安全度評価の基本枠組やその拡張を提案した。要素技術として配信者の不正も考慮して配信者が勝手に排除対象を決めることができない機能やブラックボックス型の不正者追跡機能をもつ配信法を開発した。さらに、安全性が保証されている配信方式において配信効率を改善した。

平成14年度は、前年度提案した放送型コンテンツ配信法の実装実験、楕円曲線上のペアリングを用いた落とし戸付き分離不能多重化通信方式とその有料コンテンツ配信への応用、XMLで記述されたコンテンツの統合を中心とした研究を行い、以下のような成果を得た。放送型コンテンツ配信法の実装実験では、効率上最も問題となるクライアントでのセッション鍵復号時間を評価した。その結果、加入者総数が1万人程度の場合でも十分実用的であることがわかった。落とし戸付き分離不能多重化通信については、一つの方式を提案し、有料コンテンツ配信への応用を示した。この有料配信システムは定額制を基本とするが最初の試用期間は従量制を利用することができ、定額制への移行が容易に行なえるという特長をもつ。XMLで記述されたコンテンツの統合については、複数の組織によってXMLデータが提供される環境を想定し、それらのデータの配信を統一的行なえるための枠組について考察した。

平成15年度は、複雑度と安全性の関係を考慮したコンテンツの配信管理法に関して研究を行い、分岐構造をもつコンテンツの配信や視聴動向調査を含む配信を対象として安全性の仮定と複雑度の関係を調べた。

また、XML で記述されたコンテンツが増加しているという背景をうけて、アクセス制御ポリシーが規定された XML 文書におけるビューを切り出すプログラムを自動生成するツールの開発を行った。さらに、プロトコルに対する安全性保証に関する研究として、コンテンツ配信管理に関する様々な機関や人に対して、配信管理法の安全性をわかりやすく示す技術の開発を行った。

平成 16 年度は、コンテンツ配信管理システムとその安全性について以下のような研究を行った。コンテンツ配信管理システムでは、インタラクティブドラマの配信に関して携帯電話のように通信事業者が仲介者として関与できる環境における配信法を提案した。また、コンテンツの委託配信において、ユーザのプライバシー保護、取引状況の委託先への秘匿販売、販売者（委託元）が取引状況を把握できること等を満たすプロトコルの提案を行った。また、オブジェクト指向データベースへの推論攻撃の安全性の判定可能性などの結果を得た。推論攻撃とは、ユーザが実行を許可された問合せのみを用いて、許可されていない問合せの実行結果に関する情報を推論して得ようとすることである。また、一般の暗号プロトコルについて、それが安全でないときに、コスト最小攻撃の導出法も求めた。

平成 17 年度は、前年度に引き続く研究以外に、時間限定サービスに関する研究を行った。コンテンツ配信サービスには、ユーザがコンテンツを利用可能な時間をコントロールするようなサービス形態がある。これを時間限定サービスと呼ぶ。時間限定サービスにおいて、ユーザの個人情報を守り、時間限定サービス特有の安全性要求を満たす方式を二つ提案した。また各方式に要求される複雑さを分析した。

前年度に引き続く研究として、インタラクティブドラマの配信とその安全性、推論攻撃による情報漏洩の不可能性検証を行った。これまでの推論攻撃に関する研究のほとんどは等価性推論（すなわち、許可されていない問い合わせの実行結果そのものを求める推論）に注目していた。しかし、非等価性推論（すなわち、許可されていない問い合わせの実行結果になり得ない値を求める推論）により機密情報が脅威にさらされる場合も多く存在する。そこで、オブジェクト指向データベースにおける非等価性推論に関して 2 種類の安全性判定問題を定義し、それぞれの計算複雑さを求めた。

2 研究期間と研究経費の配分額

本研究は、平成 13 年度より 17 年度までの 5 年間に渡って進められた。この間に配分された研究経費は下記のとおりである。

年度（平成）	13	14	15	16	17	合計
研究費（千円）	6,000	6,000	5,300	6,000	5,400	28,700

また、課題番号と課題名は以下の通りである。

13 年度	13224063	コンテンツ配信管理システムに関する統合的セキュリティ技術の研究
14 年度	14019060	コンテンツ配信管理システムに関する統合的セキュリティ技術の研究
15 年度	15017259	コンテンツ配信管理における複雑度と安全性のトレードオフ及び安全性保証に関する研究
16,17 年度	16016258	コンテンツ配信管理システムとその安全性確認に関する研究

3 研究成果

以下では、今年度行った研究を中心に成果のうちのいくつかを紹介する。コンテンツ配信管理システムの開発に関する研究としては分岐構造をもつコンテンツの配信について、コンテンツ配信管理に役立つ要素技術に関する研究として時間限定サービスについて述べる。また、コンテンツ配信管理の安全性に関する研究としてはオブジェクト指向データベースにおける非等価性推論の不可能性検証法について述べる。

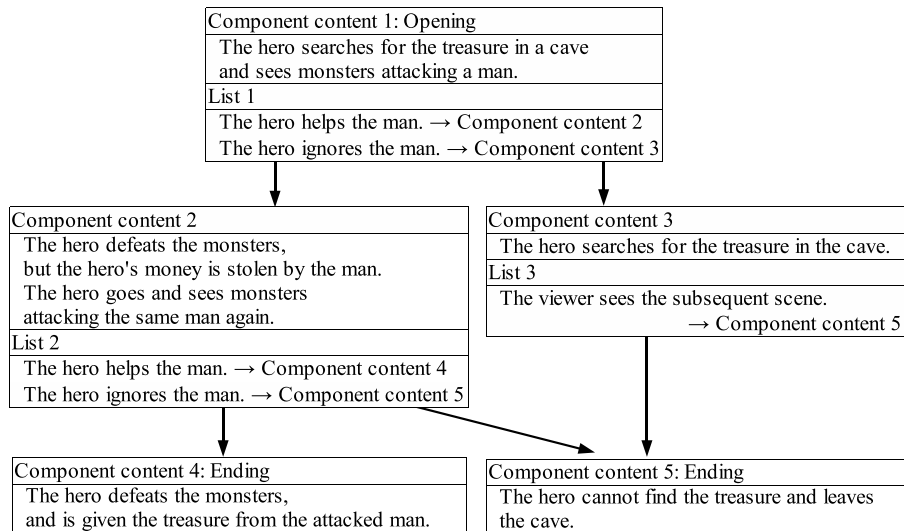


図 1: インタラクティブドラマの例

3.1 分岐構造をもつコンテンツの配信

コンテンツ配信サービスが多様化し、様々な論理的構造をもつコンテンツの配信が行なわれている。論理的構造をもつコンテンツの例として、インタラクティブドラマと呼ばれる動画コンテンツが挙げられる。ドラマは、ストーリーの整合性（流れ）が保たれつつ、その途中で示される分岐選択肢（以下、選択肢）から何を選択するかによって、その後のストーリー展開が異なるように配信される。今後、このような分岐構造をもつコンテンツの配信がより盛んになると考えられる。

コンテンツ利用者のプライバシー保護への意識が高まるに伴い、利用者に関してコンテンツ配信者が得る情報が利用料金の請求やマーケティングなどの正当な目的のために必要となる情報だけであることを保証できることは重要となっている。インタラクティブドラマの配信では、選択肢によって、利用者の嗜好や性格が選択に強く反映されると考えられる。よって、利用者がどのようなストーリーを見たかを表す情報（その利用者の選択履歴）は配信者に知られないことが望ましい。

従来、コンテンツ利用者の購入に関するプライバシー保護は、電子商取引方式 [1]、電子現金方式 [2]、anonymous fingerprinting 方式 [3, 4] などと考えられていた。しかし、対象とするコンテンツは構造をもっておらず、構造に応じた配信制御はこれまでに扱われていない。

そこで、本研究では、配信者が分岐構造をもつコンテンツの配信を制御でき、かつ利用者のプライバシーが保護される配信システムを提案する。提案システムでは、配信者は各項目の選択回数を正しく把握できる。しかし、全ての選択履歴の中で、どれが同一の利用者によるものが、自明な場合を除いて特定できない。これにより、システム外からの情報で、ある利用者について一部の選択履歴が配信者に知られてしまった場合でも、その利用者のそれ以外の選択については配信者に知られない。

3.2 オブジェクト指向データベースにおける非等価性推論の不可能性検証

これまでに、オブジェクト指向データベースに関する様々なアクセス権モデルが提案されている。その中に、オブジェクトにはメソッド（問合せプログラム）を用いてのみアクセス可能であるというモデルがある [13, 16]。このモデルでは、ユーザ u に対するアクセス権 A は u が直接実行できるメソッド全体の集合として表される。しかし u が A に含まれるメソッドのみを用いて、 A に含まれていないメソッドの実行結果に関する情報を間接的に得ることが可能な場合がある。一般に、データベースにおいて、ユーザ u が非許可の問合せ τ の実行結果に関する情報を推論により得ようとするを推論攻撃という。また推論攻撃の結果、

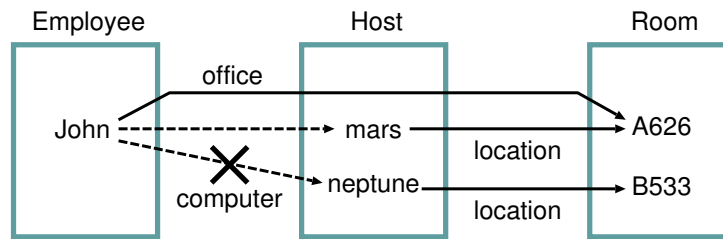


図 2: 非等価性推論可能な例

ユーザ u が, τ の実行結果に関する何らかの情報を得ることができる (あるいはできない) とき, τ は推論攻撃に対して安全でない (あるいは安全である) という. アクセス制御を行うデータベースでは, アクセス権の与えられていない問合せの実行結果が推論される可能性があることは好ましくない場合が多いため, 推論による情報漏洩の不可能性を検証することが重要である.

これまで, 本研究グループでは, オブジェクト指向データベースにおける推論の不可能性検証法を提案してきた [14, 15]. しかしこれらの検証法は, τ の実行結果そのものを求める推論 (等価性推論と呼ぶ) のみを対象にしていたため, これらの検証法で安全であると判定された場合でも, τ の実行結果になり得ない値を求める推論 (非等価性推論と呼ぶ) に対しては, データ漏洩の可能性が残されるという問題があった.

図 2 に非等価性推論が可能な場合の例を示す. Employee, Host, Room はそれぞれ従業員名, ホスト名, 部屋番号のクラスである. office, computer, location はそれぞれ従業員の部屋番号, 従業員の使用しているホスト, 各ホストの置かれている部屋番号を返すメソッドである. また office は $\text{office}(x) = \text{location}(\text{computer}(x))$ と実装されている. ユーザ u には office, location の実行が許可されており, computer の実行が許可されていないとする. まず, $\text{office}(x) = \text{location}(\text{computer}(x))$ と $\text{office}(\text{John}) = \text{A626}$ より $\text{location}(\text{computer}(\text{John})) = \text{A626}$ を得る. この結果と $\text{location}(\text{neptune}) = \text{B533}$, $\text{A626} \neq \text{B533}$ より, $\text{computer}(\text{John}) \neq \text{neptune}$ を得ることが可能である.

本年度はオブジェクト指向データベース (OODB) における非等価性推論について以下の成果を得た. まず, メソッドスキーマ [12] とよばれる OODB のモデルのもとで, 非等価性推論を形式的に定義した. 次に, 以下の 2 種類の安全性判定問題を定義した.

1. 与えられたデータベースインスタンスが非等価性推論に対して安全か?
2. 与えられたデータベーススキーマのすべてのデータベースインスタンスが非等価性推論に対して安全か?

そして, 前者の問題はデータベースインスタンスの記述長に対して多項式時間で判定可能であること, 一方後者の問題は判定不能であることを示した. 後者の問題に対してはさらに, 安全であるための判定可能な十分条件を与え, すべての問合せが 1 引数であるデータベーススキーマにおいてはこの十分条件が必要条件にもなることを示した.

3.3 時間限定サービス

時間限定サービスに対する安全性要求として, これまでに二つ考えられている. 一つは, 指定された期間だけコンテンツを利用可能とすることである [6, 9] (期間限定機能と呼ぶ). もう一つは, 指定された時刻になったときに初めてコンテンツを利用可能とすることである [5, 7, 8] (タイムカプセル機能と呼ぶ).

各機能を実現するためにコンテンツを暗号化した場合, 復号するための鍵を管理することが必要となる. 本年度は期間限定機能とタイムカプセル機能の実現する鍵管理に関して, 以下の成果を得た.

期間限定機能の実現: 妥当な鍵管理方式の提案

これまでに提案された期間限定機能をもつ鍵管理方式 [6] は、効率が良いが、必要となる暗号技術には強い制約条件があり、その制約条件を満たす具体的な暗号技術が見つかっていなかった。

よって本年度は、[9] において、想定する使用環境で妥当と考えられる安全性の高さを保証し、かつ従来よりも制約条件緩い、新しい鍵管理方式を提案した。また、制約条件を満たす暗号技術の候補を示し、提案方式の複雑さを従来方式と比較した。提案方式では、メモリ量と通信量に関しては従来法より増加したが、サービスが提供される期間や指定された期間の長さに比例せず、対数オーダーで済む。さらに、計算量に関しては従来法より削減された。

タイムカプセル機能の実現：耐性をもつ鍵管理方式の提案

これまでに提案されたタイムカプセル機能をもつ鍵管理方式のうち最も効率が良い方式 [5, 8] では、鍵管理サーバがタイムサーバとして、時刻の認証情報を放送する。ユーザはその認証情報を受信できれば復号鍵を計算できるが、認証情報を見逃すと復号鍵を計算できない。

よって本年度は、昨年度の検討結果 [10] をもとに、[11] において、ユーザの認証情報の見逃しに対する耐性を強化した鍵管理方式を提案し、その複雑さを従来方式と比較した。提案方式では、ある復号鍵のための認証情報を見逃したとしても、その後の復号鍵のための認証情報を見逃さなければ復号鍵を計算できる。提案方式では、認証情報を見逃した復号鍵の計算処理が加わったが、それ以外の処理の複雑さは従来方式と同じですむ。

3.4 今後の展望

本研究では、ここで報告したように大別して三つの分野で研究を進めた。今後の展望は以下のとおりである。

- 本研究ではコンテンツ配信形態として B2C を対象として様々な状況における安全なコンテンツ配信管理法を考案してきた。C2C も重要となりつつあり、今後は C2C における様々な要求を分析し配信管理法を開発する予定である。
- 不正防止の観点からは、PKI ベースの証明書やタイムスタンプを利用して、より便利で安全な配信管理が重要となると思われる。これらを含め、より充実したコンテンツ配信管理システムの設計を今後検討する。
- 安全性検証・確認に関する研究では、欠陥がある場合のわかりやすい指摘の方法等の成果をあげてきた。今後は、特に世間一般の利用者に安全であることを納得させるのに何が有効であるかという点によりいっそう重点をおき、研究をすすめていく予定である。
- オブジェクト指向データベースへの推論攻撃に対する安全性検証については、さまざまな問題設定のバリエーションのもとでの検証の計算複雑さを与えたという点で、一定の成果を得たと考えている。今後は、近年急速に普及しつつある XML データベースに焦点を当て、推論攻撃を定式化し、安全性検証法を開発する予定である。

参考文献

- [1] B. Aiello, Y. Ishai, and O. Reingold, “Priced Oblivious Transfer: How to Sell Digital Goods,” EUROCRYPT’01, LNCS 2045, pp.119–135, 2001.
- [2] D. Chaum, “Security without Identification: Transaction Systems to make Big Brother Obsolete,” Communications of the ACM, Vol.28, No.10, pp.1030–1044, 1985.
- [3] B. Pfitzmann and A.-R. Sadeghi, “Coin-Based Anonymous Fingerprinting,” EUROCRYPT’99, LNCS 1592, pp.150–164, 1999.

- [4] B. Pfitzmann and M. Waidner, "Anonymous Fingerprinting," EUROCRYPT'97, LNCS 1233, pp.88–102, 1997.
- [5] I.F. Blake and A.C-F. Chan, "Scalable, Server-Passive, User Anonymous Timed Release Public Key Encryption from Bilinear Pairing," <http://eprint.iacr.org/2004/211/>.
- [6] Y. Kaji and R. Nojima, "A Management Scheme of Time Series of Cryptographic Keys for Time-Limited Services," Proc. 2005 Symposium on Cryptography and Information Security, pp. 289–294, 2005.
- [7] T. May, "Timed-Release Crypto," <http://www.hks.net.cpunks/cpunks-0/1560.html>, 1992.
- [8] I. Osipkov, Y. Kim, and J.H. Cheon, "New Approaches to Timed-Release Cryptography," <http://eprint.iacr.org/2004/231/>.
- [9] M. Yoshida, Y. Kaji, and T. Fujiwara, "A Time-Limited Key Management Scheme Based on a One-Way Permutation Tree," IEICE Technical Report, IT2005-29, 2005.
- [10] M. Yoshida, S. Mitsunari, and T. Fujiwara, "Time-Capsule Encryption," 2005 Hawaii, IEICE and SITA Joint Conference on Information Theory pp.165–170, 2005.
- [11] M. Yoshida, S. Mitsunari, and T. Fujiwara, "A Timed-Release Key Management Scheme for Backward Recovery," 8th Annual International Conference on Information Security and Cryptology (Proceedings will be published as a book in LNCS), 2006.
- [12] S. Abiteboul, P. Kanellakis, S. Ramaswamy, and E. Waller, "Method schemas," Journal of Computer and System Sciences, Vol. 51, No. 3, pp. 433–455, 1995.
- [13] E.B. Fernandez, M.M. Larronodo-Peritrie, and E. Gudes, "A method-based authorization model for object-oriented databases," Proceedings of OOPSLA-93 Conference Workshop on Security for Object-Oriented Systems, pp. 135–150, 1993.
- [14] Y. Ishihara, T. Morita, and M. Ito, "The security problem against inference attacks on object-oriented databases," Research Advances in Database and Information Systems Security, pp. 303–316, Kluwer, 2000; A full version can be found at <http://www-infosec.ist.osaka-u.ac.jp/~ishihara/papers/dbsec99.pdf>.
- [15] T. Morita, Y. Ishihara, H. Seki, and M. Ito, "A formal approach to detecting security flaws in object-oriented databases," IEICE Transactions on Information and Systems, Vol. E82-D, No. 1, pp. 89–98, 1999.
- [16] H. Seki, Y. Ishihara, and M. Ito, "Authorization analysis of queries in object-oriented databases," Proceedings of the Fourth International Conference on Deductive and Object-Oriented Databases, LNCS 1013, pp. 521–538, 1995.

4 研究発表

学会誌等

1. Yasunori Ishihara, Kengo Mori and Toru Fujiwara: “Sufficient Conditions for Update Operations on Object-Oriented Databases to Preserve the Security against Inference Attacks”, *IEICE Transactions on Information and Systems*, Vol. E86-D, No. 10, pp.2187-2197, 2003.
2. Shingo Okamura, Maki Yoshida, and Toru Fujiwara: “Unlinkable Delivery System for Interactive Dramas”, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E88-A, No. 1, pp.262-269, 2005.
3. Yasunori Ishihara, Shuichiro Ako and Toru Fujiwara: “Security against Inference Attacks on Negative Information in Object-Oriented Databases”, *IEICE Transactions on Information and Systems*, Vol. E88-D, No. 12, pp.2767-2776, 2005.
4. Maki Yoshida and Toru Fujiwara: “Further Improvement of Kumar-Rajagopalan-Sahai Coding Constructions for Blacklisting Problem”, 8th IMA International Conference on Cryptography and Coding, LNCS2260, Springer-Verlag Berlin Heidelberg, pp.27-37, 2001.
5. Shingo Okamura, Maki Yoshida and Toru Fujiwara: “A Validatable Revocation Scheme with Black-Box Traitor Tracing”, 2002 International Symposium on Information Theory and Its Applications, pp.355-358, 2002.
6. Takayuki Ueno, Maki Yoshida and Toru Fujiwara: “A Method of Estimating the Detection Error Rate in a Certain Digital Watermarking for Audio Signals”, 2002 International Symposium on Information Theory and Its Applications, pp.359-362, 2002.
7. Yasunori Ishihara, Shuichiro Ako and Toru Fujiwara: “Security against Inference Attacks on Negative Information in Object-Oriented Databases”, The Fourth International Conference on Information and Communications Security, pp.49-60, 2002.
8. Yasunori Ishihara, Yumi Shimakawa and Toru Fujiwara: “Type Inferability and Decidability of the Security Problem against Inference Attacks on Object-Oriented Databases”, The 6th International Conference on Information and Communications Security, pp.145-157, 2004.
9. Akira Fujiwara, Shingo Okamura, Maki Yoshida, and Toru Fujiwara: “A Digital Contents Consignment System Protecting Marketing Information”, 2004 International Symposium on Information Theory and Its Applications, pp.468-473, 2004.
10. Shingo Okamura, Maki Yoshida and Toru Fujiwara: “Unlinkable Delivery System for Interactive Dramas Including Conditional Choices”, 2004 International Symposium on Information Theory and Its Applications, pp.474-479, 2004.
11. Kunihiro Okamoto, Takayuki Ueno, Maki Yoshida, and Toru Fujiwara: “A Method to Ensure Reliability of a Detection Result for Correlation Based Watermark Detection Schemes”, 2004 International Symposium on Information Theory and Its Applications, pp.299-304, 2004.
12. Shingo Okamura, Maki Yoshida, and Toru Fujiwara: “An Interactive Drama Delivering System Suitable for Mobile Phone”, Workshop on Information Security Applications 2004 (Pre-Proceedings), pp.391-398, 2004.

13. Shingo Okamura, Maki Yoshida, and Toru Fujiwara: “Coin-based Anonymous Fingerprinting Scheme with Automatic Identification of Redistributors”, ISSA 2005 New Knowledge Today Conference , 2005.
14. Satoshi Nakayama, Maki Yoshida, Shingo Okamura, Akira Fujiwara, and Toru Fujiwara: “An Efficient Private and Consistent Data Retrieval Protocol”, Western European Workshop on Research in Cryptology, pp.83-84, 2005.
15. Takaaki Fujita, Kunihiro Okamoto, Maki Yoshida, and Toru Fujiwara: “A Watermark Detection Scheme Ensuring the False Positive Error Probability”, Western European Workshop on Research in Cryptology, pp.18-19, 2005.
16. Maki Yoshida, Shigeo Mitsunari, and Toru Fujiwara: “A Timed-Release Key Management Scheme for Backward Recovery”, 8th Annual International Conference on Information Security and Cryptology (Proceedings will be published as a book in LNCS), 2006.

口頭発表等

1. 藤原 晶, 岡村 真吾, 吉田 真紀, 藤原 融: “コンテンツ配信サービス提供者だけが視聴動向を把握できる委託配信システム”, 2004 年暗号と情報セキュリティシンポジウム予稿集, Vol. I, pp. 487-492, 2004.
2. 藤原 晶, 岡村 真吾, 吉田 真紀, 藤原 融: “マーケティング情報が保護された委託配信システムにおける通信頻度の削減”, 電子情報通信学会技術研究報告, ISEC2004-34, 2004.
3. 藤原 晶, 岡村 真吾, 吉田 真紀, 藤原 融: “マーケティング情報が保護されたオフライン委託配信システム”, コンピュータセキュリティシンポジウム 2004 論文集, Volume II, pp. 469-474, 2004.
4. 馬山 貴峰, 吉田 真紀, 藤原 融: “暗号を用いたプロトコルに対するコスト最小攻撃の形式的導出法”, 電子情報通信学会技術研究報告, ISEC2004-87, 2004.
5. Maki Yoshida, Shigeo Mitsunari, Toru Fujiwara: “Time-Capsule Encryption”, IEICE Technical Report, ISEC2004-98, 2004.
6. 中山 敏, 藤原 晶, 吉田 真紀, 藤原 融: “検索結果の秘匿と一貫性検証を可能とするデータ検索プロトコルの提案とその応用”, 2005 年暗号と情報セキュリティシンポジウム, pp.1489-1494, 2005.
7. Maki Yoshida, Yuichi Kaji, and Toru Fujiwara: “A Time-Limited Key Management Scheme Based on a One-Way Permutation Tree”, 2005 Hawaii, IEICE and SITA Joint Conference on Information Theory, 165-170. 2005
8. 中山 敏, 吉田 真紀, 岡村 真吾, 藤原 晶, 藤原 融: “検索語の秘匿と検索結果の一貫性検証を可能とするデータ検索プロトコルにおける通信量の削減”, 電子情報通信学会技術研究報告, ISEC2005-61, 2005.
9. 吉田 真紀, 藤原 融: “先着限定販売のための売り切れ証明プロトコル”, コンピュータセキュリティシンポジウム 2005, pp.523-528, 2005.

著書・出版物

1. 藤原 融: “暗号プロトコル検証”, 電子情報通信学会, 情報セキュリティハンドブック (第3編第3章), オーム社, 2004.