

امنیت پخش تلویزیون و ویدئوی دیجیتال

تألیف:

حمیدرضا دامغانی

مدرس دانشگاه

لیلا دامغانی

مدرس دانشگاه

www.ketab.ir

سرشناسه : دامغانی، حمیدرضا، ۱۳۶۵ -

عنوان و نام پدیدآور : امنیت بخش تلویزیون و ویدئوی دیجیتال / نویسندگان حمیدرضا دامغانی، لیلا دامغانی.

مشخصات نشر : تهران: نارون دانش، ۱۳۹۸.

مشخصات ظاهری : ۸۴ص. مصور (بخشی رنگی)، جدول، نمودار (بخشی رنگی).

شابک : ۹۷۸-۶۲۲-۶۹۲۴-۵۰-۴

وضعیت فهرست نویسی : فیبا

یادداشت : کتابنامه : ص. ۵۲ - ۵۵.

موضوع : رمزگذاری داده‌ها -- الگوهای ریاضی

موضوع : Data encryption (Computer science) -- Mathematical models

موضوع : تلویزیون رقمی -- پیش‌بینی‌های ایمنی

موضوع : Digital television -- Safety measures

موضوع : تلویزیون رقمی -- الگوهای ریاضی

موضوع : Digital television -- Mathematical models

موضوع : ویدئوی رقمی -- الگوهای ریاضی

موضوع : Digital video -- Mathematical models

موضوع : ویدئوی رقمی -- داده‌های ریاضی

موضوع : Digital video -- Data processing

موضوع : تلویزیون -- فرستنده‌ها

موضوع : Television -- Transmitters and transmission

شناسه افزوده : دامغانی، لیلا، ۱۳۶۳ -

رده بندی کنگره : QA۷۶/۹

رده بندی دیویی : ۸/۰۰۵

شماره کتابشناسی ملی : ۵۸۹۵۳۳۰

آدرس: میدان انقلاب اسلامی، خیابان کارگر شمالی، زمین ندرت شقایق، پلاک هفتادودو، واحد یک

شماره تماس: 09224013704 و 021-6932222

آدرس الکترونیکی: narvanpub@gmail.com

آدرس سایت: www.narvanpub.com



عنوان کتاب: امنیت بخش تلویزیون و ویدئوی دیجیتال

مؤلفین: حمیدرضا دامغانی و لیلا دامغانی

صفحه‌آرا: اکرم ملک نژاد

طراح جلد: الویرا صیامی

ناشر: انتشارات نارون

شمارگان: ۱۰۰۰ نسخه

نوبت چاپ: اول - ۱۳۹۸

قیمت: ۲۰۰۰۰ تومان

ISBN: 978-622-6924-50-4

فهرست مطالب

۱۱	فصل اول: مقدمه
۱۴	معرفی HEAD-END
۱۵	واژه‌ی کنترل
۱۵	سیستم دسترسی مشروط
۱۶	استانداردها
۱۷	DVB-SIMULCRYPT
۱۷	رابط مشترک
۱۸	معرفی TS
۱۹	مازول دسترسی مشروط
۲۰	رمزنگاری
۲۱	چرا رمزنگاری نیاز است؟
۲۱	بسته‌های داده
۲۲	بسته‌های TS
۲۳	سرفایل
۲۴	پهنه تطابق
۲۵	Payload رمزگذاری شده و Payload خالص
۲۵	بسته‌های PES
۲۶	رمزگذاری و رمزگشایی
۲۶	رمزنگای با کلید متقارن
۲۷	رمزنگاری با کلید عمومی
۲۷	ترکیبی از روش‌های رمزگذاری
۲۹	تعریف رمز
۲۹	رمز بخشی
۳۲	رمز جریان
۳۲	رمزگشایی
۳۲	اغتشاش و انتشار
۳۳	S-box ها و P-box ها
۳۴	معرفی اختفا

۳۴	الگوریتم تکاپوی مشترک
۳۵	نیاز به یک استاندارد جدید
۳۶	ساختار CSA
۳۶	تعریف و اهمیت امنیت
۳۷	شکستن CSA
۳۷	معرفی حمله Brute force
۳۹	معرفی حمله Known plaintext
۴۰	معرفی حمله Time Memory trade off (TMT0)
۴۰	SSA یا CSA3
۴۰	جایگزین‌های الگوریتمی
۴۱	معرفی CISA
۴۲	تطبیق نرم افزاری CSA
۴۳	ساختار CSA3
۴۳	تطبیق سخت افزاری CSA3
۴۳	انتخاب الگوریتم
۴۵	فصل دوم: الگوریتم پیشنهادی
۴۷	مقدمه
۴۸	مروری بر الگوریتم تکاپوی مشترک
۴۹	بخش رمزگذاری بخشی الگوریتم تکاپوی مشترک
۵۰	معرفی تابع چرخه
۵۱	زمان‌بندی کل - اید مشترک
۵۱	رمزگذاری و رمزگشایی
۵۲	قسمت رمزگذاری الگوریتم پیشنهادی
۵۵	قسمت رمزگشایی الگوریتم پیشنهادی
۵۶	جمع بندی و نتیجه گیری
۵۷	فصل سوم: ارزیابی روش رمزگذاری پیشنهادی
۶۰	چگونگی اعمال حمله [ها]
۶۵	نتایج ارزیابی و اعمال حملات
۷۷	فصل چهارم: سخن پایانی
۸۱	فهرست منابع

پیشگفتار

الگوریتم تکاپوی مشترک (CSA)، برای رمزدار کردن جریان‌های ویدئویی در سیستم‌های بخش ویدئویی دیجیتال به کار می‌رود. برای حاشیه‌ی امنیت بیشتر، این الگوریتم به صورت ترکیب توالی رمزکننده‌ی جریان و رمزنامه‌ی بخشی می‌باشد. در این کتاب به اجرای روش ارتقا یافته‌ی از الگوریتم CSA به منظور کاهش ضریب امنیت داده‌ها پرداخته می‌شود. با ادغام همزمان چندین ارتقا در کدهای اصلی، علاوه بر بالا بردن ضریب امنیت در هسته اصلی CSA، روشی را برای حفاظت از اطلاعات نیز اجرا کردیم که به صورت دستیابی ناخواسته به این اطلاعات، ضریب امنیت بکار گرفته شده افزایش یابد. در نهایت برای بررسی بیشتر الگوریتم پیشنهادی، دو حمله‌ی TMTO و حمله‌ی Brute force را به این الگوریتم اعمال خواهیم کرد. نتایج به دست آمده نشان می‌دهند که الگوریتم پیشنهادی در مقابل این حملات بسیار مقاوم است.

آدرس ایمیل نویسنده به جهت برقراری ارتباط و بهبود مطالب

Hamidreza.damghani@gmail.com