مدل معماری ترکیبی با هدف ارتقای امنیت پرداخت های همراه در بانکداری الکترونیک

محسن اسلام نژاد، کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه تربیت مدرس،
m.eslamnezhad@modares.ac.ir
علی یزدیان ورجانی، استادیار دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس،
yazdian@modares.ac.ir

سومین همایش سالانه بانکداری الکترونیک و نظام های پرداخت

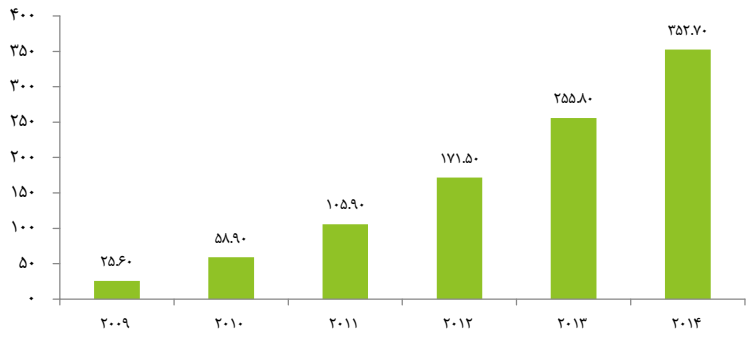
conf.mbri.ac.ir/ebps3

فهرست مطالب

مقدمه

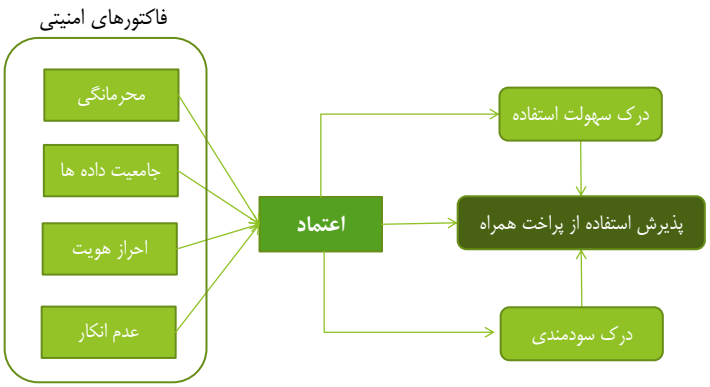
جایگاه پرداخت همراه در تجارت الکترونیک

- پیش بینی تراکنشهای پرداخت همراه در کل جهان در سال ۲۰۱۷ میلادی (موسسه گارتنر)
- ارزش کل تراکنشها برابر با ۷۲۱ بیلیون دلار
- بیش از ۴۵۰ میلیون کاربر سیستم های پرداخت همراه



مقدمه

مدل مفهومی اعتماد کاربر و پذیریش پرداخت همراه



مقدمه

ویژگی های امنیتی مورد نیاز پرداخت همراه

- پروتکلهای پرداخت الکترونیک (SET، 3KP، Tellez، KSLv1، KSLv2)

محرمانگی	جامعیت	احراز هویت	عدم انکار
رمزنگاری نا متقارن (کلید عمومی) رمزنگاری متقارن	توابع درهم سازی امضای دیجیتال	کلید متقارن امضای دیجیتال PIN روشهای بیومتریک	امضای دیجیتال MAC

رمزنگاری به عنوان رکن اصلی فاکتورهای امنیتی

مقدمه

تعریف مسئله

- **مسئله**
  - نیاز به ارتقا امنیت پرداختهای همراه به منظور کاهش آسیب پذیریهای موجود و در نتیجه افزایش اعتماد کاربران
  - عدم بهره گیری مؤثر از تکنیک های رمزنگاری با توجه به محدودیت توان پردازش و حافظه مصرفی ابزار های همراه
- **اهداف پژوهش**
  - ارائه مدل معماری باا استفاده از الگوریتمهای رمزنگاری خم بیضوی و خلاصه پیام BLAKE2 به منظور ارتقا امنیت پرداخت همراه با توجه به محدودیت منابع ابزارهای همراه

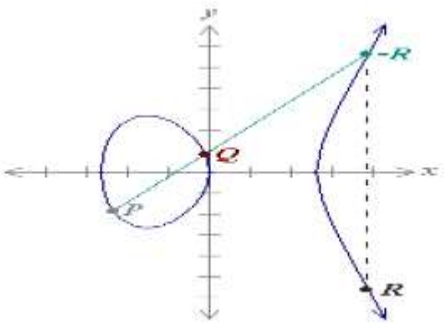
پیشینه پژوهش

نام نویسندگان	سال	موضوع
Großschädl, J., Page, D., & Tillich, S.	۲۰۱۲	پیاده سازی مؤثر الگوریتم رمزنگاری خم بیضوی با استفاده از زبان Java به منظور استفاده در ابزارهای همراه
Ganesan, S. P.	۲۰۱۱	ارائه پروتکل احراز هویت با استفاده از الگوریتم رمزنگاری HECC به منظور استفاده در ابزارهای همراه
Abdurahmonov, T., Yeoh, E. T.	۲۰۱۱	ارتقا امنیت کارتهای هوشمند با استفاده از الگوریتم رمزنگاری ECC
Ganesan, R., & Vivekanandan, K	۲۰۰۹	ارائه یک مدل معماری ترکیبی به منظور استفاده در بانکداری اینترنتی
Ganesan, M. S. P	۲۰۰۹	پروتکلی کارا با استفاده از الگوریتم ECC برای پلتفرمهایی با منابع محدود
Ganesan, R., Gobi, M., & Janakiraman, V. S	۲۰۰۸	پیاده سازی مکانیزم MD5 Integrity Checking برای تراکنشهای تجارت همراه

رمزنگاری خم بیضوی

کلیات خم بیضوی

- یک شی ریاضی با ویژگیهای خاص
- خم بیضوی روی اعداد حقیقی، مجموعه‌ای از نقاط (x, y) در معادله خم بیضوی
- معادله خم بیضوی $y^2 = x^3 + ax + b$



رمزنگاری خم بیضوی

مسئله لگاریتم گسسته خم بیضوی

- با نقاط داده شده Pو Q، مسئله لگاریتم گسسته خم بیضوی، یافتن یک مقدار Kاست بطوریکه PK= Q.
- عدم ارائه الگوریتمی کارا برای حل مسئله لگاریتم کسسته خم بیضوی
- استفاده از دشواری حل مسئله لگاریتم گسسته، در تولیدکلیدهای عمومی و خصوصی در سیستمهای رمزکلید عمومی
- استفاده از کلیدهای با طول کمتر با توجه به ارائه سطح امنیتی مشابه با الگوریتم های دیگر
- سریعتر از الگوریتم های رمزنگاری مشابه
- مناسب به منظور استفاده در ابزارهای همراه با توان و حافظه پردازشی محدود

طول کلید AES	طول کلید RSA	طول کلید ECC
۸۰	۱۰۲۴	۱۶۰
۱۱۲	۲۰۴۸	۲۲۴
۱۲۸	۳۰۷۲	۲۵۶
۱۹۲	۷۶۸۰	۳۸۴
۲۵۶	۱۵۳۶۰	۵۱۲

رمزنگاری خم بیضوی

رمزنگاری و رمزگشایی

- فرضیات
  - کلید خصوصی فرستنده k و کلید عمومی آن G*k.
  - کلید خصوصی گیرنده b و کلید عمومی آن G*b.
- رمزنگاری
  - فرستنده با در اختیار گرفتن کلید عمومی گیرنده (G*b)، مقدار k * (G*b) محاسبه می‌کند.
  - فرستنده، پیام m را به مقدار محاسبه شده در مرحله قبل اضافه می‌کند. c= m + G * (kb).
  - فرستنده، کلید عمومی خود و مقدار **c** را در قالب (G * k, c) برای گیرنده ارسال می‌کند.
- رمزگشایی
  - گیرنده پس از دریافت پیام رمز، مقدار G * (kb) محاسبه می‌کند.
  - گیرنده مقدار محاسبه شده در مرحله قبل را به شکل G * (kb) - قرینه می‌کند.
  - در نهایت گیرنده به منظور رمزگشایی پیام اصلی مقدار m= c + (-G * (kb)) را محاسبه می‌کند.

خلاصه پیام BLAKE2

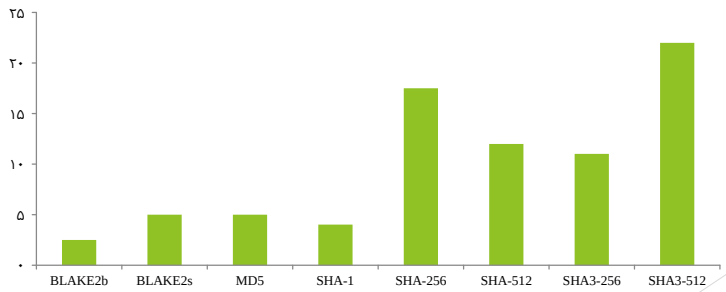
الگوریتم BLAKE و ویژگی های آن

- آسیب پذیری الگوریتم MD5 و SHA-1 بدلیل مشکل تصادم و حملات گسترده به الگوریتم SHA-1
- فراخوان طراحی الگوریتم درهم سازی SHA-3 در قالب یک مسابقه توسط NIST
- اعلام پنج الگوریتم BLAKE، Grøstl، JH، Keccak و Skein به عنوان الگوریتم‌های برتر از مجموع ۶۴ الگوریتم و پس از سه مرحله رقابت در مدت ۵ سال
- BLAKE، یکی از ساده ترین طراحی‌های توابع درهم‌سازی
- انواع الگوریتم BLAKE: BLAKE-224، BLAKE-256، BLAKE-384، BLAKE-512
- عدم ارائه گزارش حمله موفقیت آمیز، به انواع الگوریتم BLAKE

خلاصه پیام BLAKE2

مقایسه الگوریتم BLAKE2 با الگوریتم های دیگر

- نیاز به افزایش سرعت در الگوریتم های درهم سازی و ارائه الگوریتم BLAKE2
- الگوریتم BLAKE2 سریع‌تر از الگوریتم MD5
- حافظه مصرفی آن حدوداً ۳۳ درصد کمتر از الگوریتم‌های SHA-1 و SHA-2
- BLAKE2b (و یا BLAKE2) برای پلتفرم های۶۴ بیتی، شامل NEON و ARM ها
- BLAKE2s برای پلتفرم های ۸ تا ۳۲ بیتی

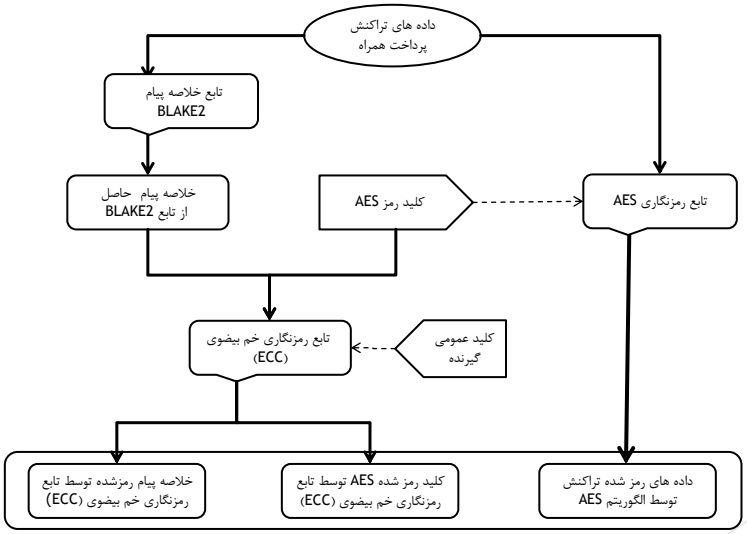


الگوریتم رمزنگاری AES

- الگوریتم رمزنگاری متقارن
- با هدف ارتقای امنیت الگوریتم رمزنگاری Triple DES توسط NIST
- طراحی آن بر مبنای رمز Rijndael
- کلیدهایی با طول‌های متفاوت ۱۲۸، ۱۹۲، و ۲۵۶
- بلاک های ۱۲۸ بیتی

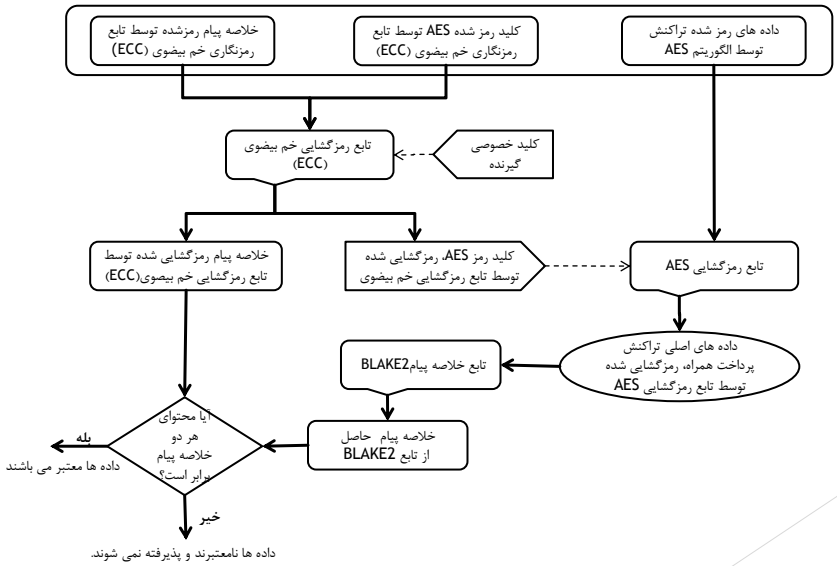
مدل معماری پیشنهادی

فرآیند رمزنگاری و ارتباط اجزای آن



مدل معماری پیشنهادی

فرآیند رمزگشایی و ارتباط اجزای آن



پیاده سازی

جزئیات پیاده سازی

- پلتفرم J2ME به همراه SDK 3.2 و چارچوب CLDC 1.1
- بهره گیری از توابع و کلاس‌های موجود در SATA API برای الگوریتم های ASE، RSA، SHA-1 و MD5
- پیاده سازی الگوریتم های رمزنگاری خم بیضوی و خلاصه پیام BLAKE2 به صورت جداگانه
- طول کلیدها بر مبنای استاندارد NIST

نتایج

زمان محاسبه رمزنگاری و رمزگشایی الگوریتم AES

اندازه فایل	رمزنگاری AES	رمزگشایی AES
۱۰ کیلو بایت	۶	۵
۳۰ کیلو بایت	۱۲	۱۰
۶۰ کیلو بایت	۱۴	۱۲

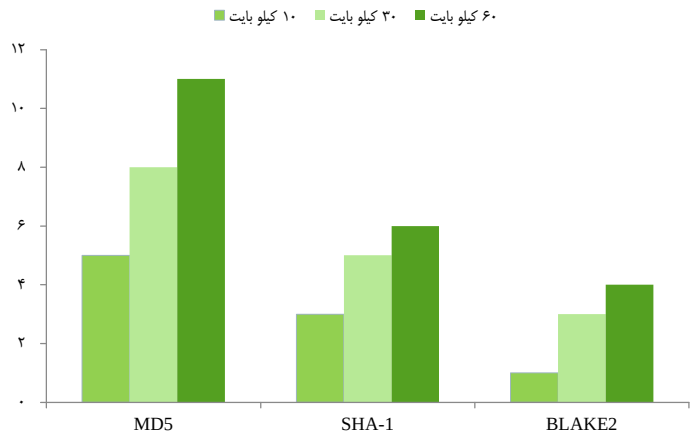
نتایج

زمان پردازش الگوریتم های MD5، SHA-1 و BLAKE2

اندازه فایل	MD5	SHA-1	BLAKE2
۱۰ کیلو بایت	۵	۳	۱
۳۰ کیلو بایت	۸	۵	۳
۶۰ کیلو بایت	۱۱	۶	۴

نتایج

مقایسه زمان اجرای الگوریتم های MD5، SHA-1 و BLAKE2



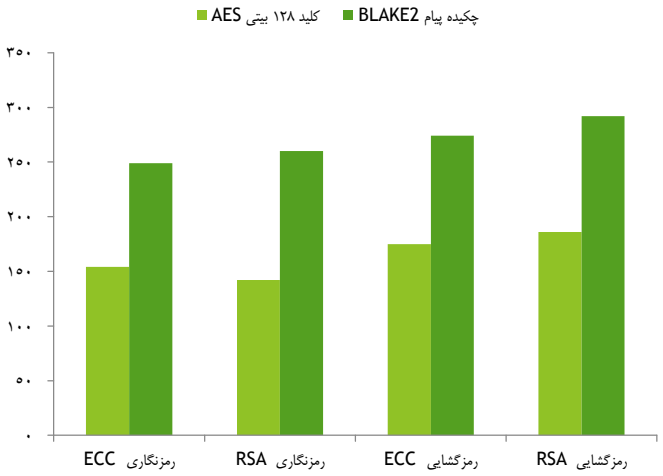
نتایج

زمان محاسبه رمزنگاری و رمزگشایی الگوریتم های ECCو RSA

	رمزنگاری ECC	رمزنگاری RSA	رمزگشایی ECC	رمزگشایی RSA
کلید ۱۲۸ بیتی AES	۱۵۴	۱۴۲	۱۷۵	۱۸۶
چکیده پیام BLAKE2	۲۴۹	۲۶۰	۲۷۴	۲۹۲

نتایج

مقایسه زمان رمزنگاری و رمزگشایی الگوریتمهای ECCو RSA



نتیجه گیری و جمع بندی

- نیاز به ارتقای امنیت مورد نیاز پرداخت‌های همراه در بانکداری الکترونیک با توجه به محدودیت توان پردازشی و حافظه مصرفی ابزارهای همراه
- ارائه مدلی ترکیبی با استفاده از الگوریتم های رمزنگاری خم بیضوی و خلاصه پیام BLAKE2
- پیاده سازی عناصر مدل با بهره گیری از ویژگیهای J2ME
- عملکرد موثر و کاراتر نسبت به روش‌های رایج
- ارتقای کیفی نیازمندی‌های امنیتی به ویژه محرمانگی و صحت داده‌ها در انتقال داده‌های حساس تراکنشهای پرداختهای همراه

منابع

[1] Kabir, G., & Akhtar Hasin, A. (2011). Evaluation of customer oriented success factors in mobile commerce using fuzzy AHP, *Journal of Industrial Engineering and Management,* 4(2), 361-386.

[2] Cottam, C. (2013), E-Commerce, *UW-L Journal of Undergraduate Research XVI.*

[3]Nambiar, S., Lu, C. T., & Liang, L. R. (2004, November). Analysis of payment transaction security in mobile commerce. In Information Reuse and Integration, 2004. IRI 2004. Proceedings of the 2004 IEEE International Conference on (pp. 475-480). IEEE.

[4]Kungpisdan, S. (2005). Modelling, Design, and Analysis of Secure Mobile Payment Systems (Doctoral dissertation, Monash University).

[5] Kumar, S. B. R., Rabara, S. A., & Martin, J. R. (2009, December). A system model and protocol for Mobile Payment Consortia System. In Test and Measurement, 2009. ICTM'09. International Conference on (Vol. 2, pp. 438-442). IEEE.

[6]Eze, U. C., Gan, G. G. G., Ademu, J., & Tella, S. A. (2008). Modelling User Trust and Mobile Payment Adoption: A Conceptual Framework .Communications of the IBIMA, 3, 224-231.

[7]Ganesan, R., & Vivekanandan, K. (2009, October). A Novel Hybrid Security Model for E-Commerce Channel. In Advances in Recent Technologies in Communication and Computing, 2009. ARTCom'09. International Conference on (pp. 293-296). IEEE.

[8]Ganesan, M. S. P. (2009). An Efficient Protocol for Resource Constrained Platforms Using ECC. International Journal on Computer Science and Engineering, 2(1), 89-91.

[9]Ganesan, S. P. (2010, March). An asymmetric authentication protocol for mobile devices using elliptic curve cryptography. In Advanced Computer Control (ICACC), 2010 2nd International Conference on (Vol. 4, pp. 107-109). IEEE.

[10]Ganesan, S. P. (2011). An Authentication Protocol For Mobile Devices Using Hyperelliptic Curve Cryptography. ACEEE International Journal on Network Security, 2(1).

[11]Ganesan, R., & Vivekanandan, K. (2009). A secured hybrid architecture model for Internet banking (e-Banking). Journal of Internet Banking and Commerce,14(1), 1-17.

[12]Gobi, M., & Vivekanandan, K. (2009). A new digital envelope approach for secure electronic medical records. IJCSNS, 9(1), 1.

[13]Ganesan, R., Gobi, M., & Janakiraman, V. S. (2008). Implementation Of MD5 Integrity Checking Mechanism For m-Commerce Transactions. International Journal of Computer Science and Applications, 1(3).

منابع

[14]Abdurahmonov, T., Yeoh, E. T., & Hussain, H. M. (2011). Improving smart card security using elliptic curve cryptography over prime field (F p). In Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing 2011 (pp. 127-140). Springer Berlin Heidelberg.

[15]Großschädl, J., Page, D., & Tillich, S. (2012). Efficient java implementation of elliptic curve cryptography for J2ME-Enabled mobile devices. In Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems (pp. 189-207). Springer Berlin Heidelberg.

[16]Babel, A. "Elliptic Curve Cryptography," F090740, Universiteit Utrecht, INFOB3CRP – Cryptography.

[17] Marshall, A. (2006) "Elliptic Curve Cryptography What is it good for ?," CSEP 590.

[18]Lotfi, A. (2013) Proposed new solution for increasing the efficiency and security in mobile payments. Master's thesis, Shahed University, Iran.

[19]Li, W., Wen, Q., Su, Q., & Jin, Z. (2012). An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network. Computer Communications, 35(2), 188-195.

[20] Babel, A. "Elliptic Curve Cryptography," F090740, Universiteit Utrecht, INFOB3CRP – Cryptography.

[21]Athale, R., & Winkler, F. (2002). Curves in Cryptography. month.

[22]Andreeva, E., Luykx, A., & Mennink, B. (2013, January). Provable security of BLAKE with non-ideal compression function. In Selected Areas in Cryptography(pp. 321-338). Springer Berlin Heidelberg.

[23]Perlner, R., Burr, W. E., Turan, M. S., Kelsey, J. M., Paul, S., & Bassham, L. E. (2012). Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition. US Department of Commerce, National Institute of Standards and Technology.

[24]Chang, D., Nandi, M., & Yung, M. (2011). Indifferentiability of the Hash Algorithm BLAKE. IACR Cryptology ePrint Archive, 2011, 623.

[25] Li, W., Wen, Q., Su, Q., & Jin, Z. (2012). An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network. Computer Communications, 35(2), 188-195. [20] Babel, A. "Elliptic Curve Cryptography," F090740, Universiteit Utrecht, INFOB3CRP – Cryptography.

[26]Aumasson, J. P., Neves, S., Wilcox-O'Hearn, Z., & Winnerlein, C. (2013). BLAKE2: simpler, smaller, fast as MD5. a preprint of the article published in the proceedings of ACNS 2013 (Springer, LNCS series)

[27]Aes, N. I. S. T. (2001). Advanced encryption standard. Federal Information Processing Standard, FIPS-197, 12.

[28]Barker, E., Barker, W., Burr, W., Polk, W., & Smid, M. (2012). Recommendation for key management–part 1: General (revision 3). NIST special publication, 800, 57.

با تشکر

سومین همایش سالانه بانکداری الکترونیک و نظام های پرداخت

۱۶ و ۱۷ دی ماه ۱۳۹۲ - مرکز همایش های برج میلاد

conf.mbri.ac.ir/ebps3