PUBLISHABLE SUMMARY

The main goal of this project is to provide security and privacy to constrained mobile devices by making efficient, tamper-resilient and robust public key cryptography (PKC) available to them. In order to accomplish this goal, this project has the following specific objectives:

1) Finding efficient finite field representations, arithmetic algorithms and hardware architectures for PKC in constrained mobile devices,
2) Efficient, low-power and tamper-resilient realization of standard public-key cryptographic schemes such as ECC and RSA , as well as more recent schemes such as Pailier's encryption and pairing based encryption, etc., for constrained mobile devices,
3) Finding new techniques for building robust cryptographic hardware operating in the frequency domain through the use of a design-for-test approach based "IC fingerprinting methodology" for the detection of hidden hardware Trojans.

With this project, Dr. Baktir's academic development and the transfer of his knowledge and experience to Europe is achieved through teaching as well as research. The researcher has taken part in active collaborations with both the academia and industry. He has maintained a lasting co-operation with the third country, and trained young researchers/students through courses, seminars and advanced degrees. As part of this project, Dr. Baktir formed collaborations with researchers both in Turkey and around Europe.

A project website, that includes the objectives, description of work done, publications, dissemination activities and information on Dr. Baktir's research group, is prepared and can be located at http://akademik.bahcesehir.edu.tr/selcuk/NDETcryptoUC.html .

Dr. Baktir investigated the application of the number theoretic transform (NTT) to finite field multiplication with an emphasis on ECC. The results of his work were present with a paper in the Fq10 conference in Belgium in 2001. He showed with both theoretical and implementation results that, particularly in computationally constrained platforms, multiplication of finite field elements can be achieved more efficiently in the frequency domain for operand sizes relevant to ECC. In order to see also the software performance of frequency domain arithmetic over constrained platforms, his research group implemented GF(p^{13}) multiplication, for $p = 2^{13} - 1$, for the constrained MSP430 microcontroller without hardware multiplier support. Their implementation of multiplication in the frequency domain, for practical operand sizes for ECC, resulted in a 100% speedup compared to classical schoolbook mutiplication. A resulting paper, titled "*Frequency Domain Montgomery Multiplication for Elliptic Curve Cryptograpy*," is submitted for publication.

Dr. Baktir conducted research on efficient software implementation of ECC in the frequency domain. He presented implementations on MSP430, a constrained microcontroller widely used in wireless sensor networks (WSN). His research resulted in the first study in the literature that presents a practical software implementation of ECC in the frequency domain. In Dr. Baktir's ECC implementations, the ECC scalar point multiplication operation was achieved in only 1.55 s and 0.77 s for random and fixed points, respectively. Furthermore, Dr. Baktir's resulting ECC implementations in the frequency domain for low-power applications, which do not utilize hardware multiplier support, were only around 20% slower. These preliminary results prove the potential of frequency domain arithmetic for constrained low-power implementations of ECC. The results of this research has been published in the paper titled "*Elliptic Curve Cryptography on Constrained Microcontrollers Using Frequency Domain Arithmetic*," presented at the 14th International Conference on Computational Science and Its Applications (ICCSA 2014) in Portugal and published in Springer Computational Science and Its Applications, Part IV, 2014. Another paper titled "*Elliptic Curve Cryptography on Low-Power Microcontrollers without Hardware Multiplier Support*" has been submitted for publication at Sensors Journal.

The researcher collaborated with Assoc. Prof. Dr. Lejla Batina (Radboud University, the Netherlands) and Assoc. Prof. Dr. Nele Mentens (Katholieke Universtaet Leuven, Belgium) on the first ever implementation of ECC using Edwards coordinates in the frequency domain. This work resulted in an efficient hardware implementation and a paper, titled "*An Elliptic Curve Cryptographic Processor Using Edwards Curves and the Number Theoretic Transform*," submitted to a conference. In this work, the researchers proposed a hardware architecture for ECC using Edwards curves and the NTT. Their design is optimized on area and explores new avenues in finding compact ECC implementations for pervasive security with improved side-channel resistance. The implementation results, with only 644 FPGA slices and 1981 LUTs for 169 bit ECC, proved to be a viable option for embedded security applications that require public-key solutions. The researchers also investigated extremely low area implementations of ECC using the same approach, but this time utilizing the available SRAM blocks on FPGA circuits. The resulting paper titled "*An Efficient Elliptic Curve Cryptographic Processor in the Frequency Domain Using SRAM Blocks on FPGA*" is in preparation for submission to a journal.

In his collaboration with Assoc. Prof. Dr. Erkay Savas (Sabanci University), Dr. Baktir proposed a new parallel Montgomery multiplication algorithm which exhibits up to 39% better performance than the known best serial Montgomery multiplication variant for the bit-lengths of 2048 or larger. Furthermore, for bit-lengths of 4096 or larger, the proposed algorithm exhibits better performance by utilizing multiple cores available, providing speedups of up to 81% and 3.37 times for microprocessors with 2 and 4 cores, respectively. This is the first work that shows that Montgomery multiplication can be practically and scalably parallelized on multi-core processors. Dr. Baktir's work was presented in the 27th International Symposium on Computer and Information Sciences (ISCIS 2012) and published in Springer Computer and Information Sciences, Volume III, 2013.

In collaboration with Dr. Naomi Benger (University of Versailles, France), Dr. Baktir examined the underlying arithmetic necessary for achieving efficient pairing computations, namely arithmetic in $GF(p^k)$ for p a prime and k a power of 3. He presented efficient representations of the required finite fields (constructed directly and quickly given the curve parameters) in order to achieve inversion and multiplication efficiently. Efficient arithmetic algorithms and finite field representations is necessary for the practical use of pairing based cryptography to eliminate the need for a Public Key Infrastructure (PKI) in constrained mobile devices. The result of this research was presented with a paper in the Fq10 conference in Belgium in 2011.

In collaboration with Dr. Tansal Gucluoglu (Yildiz Technical University) and Atilla Ozmen (Kadir Has University), Dr. Baktir developed techniques for IC fingerprinting using signal processing techniques such as the wavelet transform and spectrograms on the power side-channel signals. By catching the time-scale differences and time-frequency activities introduced by the hidden Trojans, these techniques have succesfully detected Trojans that are smaller than 1% of the total circuit area. The result of this research is presented with a paper published in the IEEE Proceedings of the International Symposium on Innovations in Intelligent Systems and Applications (INISTA 2012). Furthermore, with his collaborators, Dr. Baktir wrote another paper titled "*Artificial Neural Networks and Machine Learning for Trojan IC Detection*" that is in preparation for submission to a journal. In this work, the researchers showed that, by training an artificial neural network over power consumption signals obtained from genuine ICs, it is possible to differentiate ICs with hidden Trojans, with a success rate of over 90%, for inserted Trojans with size less than 1% of the genuine IC.

Dr. Baktir actively disseminated his knowledge through seminars, courses, senior projects and thesis/dissertation supervision. At Bahcesehir University, he developed and thought the courses "*CMP 4321 Introduction to Network Security and Cryptography*" (Fall 2011 and Summer 2014) at the senior undergraduate level, and "*CMP 5121 Network Security and Cryptography*" (Spring 2013, Fall 2013 and Spring 2014), "*CMP 6122 Advanced Topics in Cryptography*" (Spring 2013), "*CMP 6008 Directed Research in Cryptography I*" and "*CMP 6009 Directed Research in Cryptography II*" at the graduate level. As a guest lecturer at Isik University, Istanbul, he developed and thought the graduate courses titled "*CSE 513 Advanced Algorithms*" (Fall 2010) and "*CSE 546 Cryptography and Data Security*" (Spring 2011). At Bahcesehir University, in addition to teaching courses, Dr. Baktir guided

senior undergraduate and graduate students in research. He supervised senior graduation projects on the implementation of RSA, ECC and Paillier cryptographic schemes.

Dr. Baktir took part in the organization of the educational event "*2011 TUBITAK-BILGEM Cryptology Summer School for University Students*" and contributed with two seminars titled "*Factorization Algorithms and Their Applications in Cryptography*" and "*Elliptic Curves and Their Applications in Cryptography*." He also took part in the organization of the educational event *2013 TUBITAK-TUSSIDE Cryptology Days* and contributed with the seminar titled "*Techniques for Trojan Detection and Hardware Integrity.*"

Through particularly the courses "*CMP 5121 Network Security and Cryptography*" and "*CMP 6122 Advanced Topics in Cryptography*" he offered at Bahcesehir University, Dr. Baktir identified graduate students who were interested in doing research and/or conducting thesis/dissertation work in cryptography and information security. Dr. Baktir attracted full-time graduate students, as well as part-time graduate students from the industry, to conduct research in cryptography and network security. He has been supervising 5 of these students for their Ph.D. dissertations and 2 of them for their M.Sc. theses.

Dr. Baktir has developed the curriculum for the Master of Science Program in Cyber Security (http://cybersecurity.bahcesehir.edu.tr) at Bahcesehir University and has been serving as the founding director of the program since Fall 2013. This is the first ever M.Sc. program in cyber security in Turkey and already has attracted more than 20 students.

Having built a strong research network through this project, Dr. Baktir took part in a team of researchers and was awarded a research grant on finding efficient techniques for Trojan IC detection, under the TUBITAK 1007 Programme, securing over €754,000 for research. This additional grant will complement Dr. Baktir's Marie Curie Project by paying for the foundation of laboratories for developing both invasive and noninvasive techniques for Trojan IC detection and testing potential robustness of frequency domain cryptographic hardware against Trojan insertion.

Since 2013, Dr. Baktir has taken part in two Horizon 2020 ICT COST actions as a management committee member, representing Turkey. These actions are COST Action IC1306 "Cryptography for Secure Digital Interaction" and COST Action IC1204 "Trustworthy Manufacturing and Utilization of Secure Devices." Through his participation in these COST actions, Dr. Baktir has been in close contact with researchers throughout Europe.