Appendix A
Universal-2 Hash Functions

Universal hash refers to a technique that randomly choose a hash function from a class of hash functions, so that the hash output can avoid hash collision as much as possible for an arbitrary or even adversarially constructed input distribution. More precisely, for any fixed input x, if hash function $h(\cdot)$ is randomly chosen from a universal hash function class $\mathscr{H}$, then $h(x)$ is a uniformly distributed random variable.

Universal-2 hash is sometimes called 2-independent universal hash or pairwise independent universal hash. It means for any distinct but fixed x_1 and x_2, $h(x_1)$ and $h(x_2)$ are independent random variables. The mathematic definition of universal-2 hash function is stated as the follows.

Let $f : \mathscr{A} \to \mathscr{B}$ be a hash function that maps a larger set $\mathscr{A}$ into a smaller set $\mathscr{B}$. x and y are elements in $\mathscr{A}$. $\delta_f(\cdot, \cdot)$ is a collision indicator function.

$$\delta_f(x, y) = \begin{cases} 1 \ x \neq y, \ f(x) = f(y) \\ 0 \ \textit{otherwise} \end{cases} \tag{A.1}$$

Let $\mathscr{F}$ be a class of hash functions from $\mathscr{A}$ to $\mathscr{B}$. $\delta_{\mathscr{F}}(\cdot, \cdot)$ is defined as

$$\delta_{\mathscr{F}}(x, y) = \sum_{f \in \mathscr{F}} \delta_f(x, y). \tag{A.2}$$

$\mathscr{F}$ is a *universal-2* class of hash functions if for all $x, y \in \mathscr{A}$,

$$\delta_{\mathscr{F}}(x, y) \leq \frac{|\mathscr{F}|}{|\mathscr{B}|}. \tag{A.3}$$

The definition of universal-2 hash functions states that for any distinctive hash inputs x and y, no more than $1/|\mathscr{B}|$ of hash functions in $\mathscr{F}$ will map them into the same hash output.

Reference [25] presented an example of universal-2 function class. Let $|\mathscr{A}| < p$ and $\mathscr{A} = \{0, \ldots, |\mathscr{A}| - 1\}$. p is a prime number. A parameterized hash function f is defined as

S. Xiao et al., *Dynamic Secrets in Communication Security*,
DOI: 10.1007/978-1-4614-7831-7,

$$f_{m,n}(x) \equiv ((mx + n) \bmod p) \bmod |\mathscr{B}|, \tag{A.4}$$

with m, n are integers and $m \neq 0$.

Let $\mathscr{F}$ be a class of hash functions defined by

$$\mathscr{F} = \{f_{m,n} | m \in \{1, \ldots, p-1\}, n \in \{0, \ldots, p-1\}\}. \tag{A.5}$$

$\mathscr{F}$ is a universal-2 hash function class.

We may further note that the hash function class $\mathscr{F}^* = \{f_{m,n} | m \in \{1, \ldots, p-1\}, n = 0\}$ is a universal function class but does not satisfy the criterion of pairwise independent.

Appendix B
Shannon Entropy and Rényi Entropy

Shannon entroy is well known as a measure to the level of randomness contained in a random variable. For a discrete random variable X that is associated with a probability distribution $p(x)$, Its Shannon entropy is

$$H(X) = -\sum_{x\in\{X\}} p(x)\log_2 p(x). \tag{B.1}$$

In the context of information theory, the level of randomness can be interpreted as level of uncertainty when treating X as an information source. Therefore, $H(X)$ also measures the uncertainty of X.

For two random variables X and Y, the conditional Shannon entropy $H(Y|X)$ is defined as

$$H(Y|X) = -\sum_{x\in\{X\}}\sum_{y\in\{Y\}} p_{X,Y}(x,y)\log_2 p_{Y|X}(y|x). \tag{B.2}$$

$H(Y)$ measures the level of uncertainty of information source Y. $H(Y|X)$ measures how much uncertainty left in Y when the information source X is given. If Y is completely determined by X, Y is fixed when X is known. Therefore in this case, $H(Y|X) = 0$. If X carries no information of Y, knowing X does not affect the uncertainty of Y. In this case, $H(Y|X) = H(Y)$. For arbitrary X and Y, we always have $H(Y|X) \leq H(Y)$.

In this monograph, conditional Shannon entropy is used to measure the secrecy level of information. Let Y be a random variable that represents a piece of information, such as a cryptographic key. X be the information gathered by adversary by all means such as through cryptanalysis or eavesdropping. $H(Y|X)$ measures the level of uncertainty that remains in Y from the adversary's view point. In another word, $H(Y|X)$ measures how much secrecy Y has against the adversary.

Rényi entropy is a generalized entropy measure. Rényi entropy of order n is defined for $n \geq 0$ and $n \neq 1$.

S. Xiao et al., *Dynamic Secrets in Communication Security*,
DOI: 10.1007/978-1-4614-7831-7,

$$H_n(X) = \frac{1}{1-n} \log_2 \left(\sum_{x \in \{X\}} (p(X = x))^n \right) \tag{B.3}$$

When $n \rightarrow 1$, Rényi entropy of order n converges to Shannon entropy. In this dissertation, we are particularly interested in Rényi entropy of order 2, which is

$$H_2(X) = -\log_2 \sum_{x \in \{X\}} (p(X = x))^2. \tag{B.4}$$

Appendix C
Proofs to Theorems in Section 6.5

Theorem 6.2 *Suppose the bit error probability of the binary symmetric channel is p_e. the receiver's uncertainty of* $\mathbf{t}$ *given* $\mathbf{r}$ *is lower bounded by*

$$H(\mathbf{t}|\mathbf{r}) \geq \mathbf{nh}(\mathbf{p_e}) - \mathbf{n}(\mathbf{1}-\mathbf{R})\mathbf{h}(\phi_{nR+\mathbf{1}}(\mathbf{p_e})), \tag{C.1}$$

with

$$h(x) = -x\log_2 x - (1-x)\log_2(1-x) \tag{C.2}$$

$$\phi_k(x) = \frac{1+(1-2x)^k}{2}. \tag{C.3}$$

Proof Firstly, we decompose Eq. (C.1).

$$\begin{aligned} H(\mathbf{t}|\mathbf{r}) &= H(\mathbf{t},\mathbf{r}) - H(\mathbf{r}) \\ &= H(\mathbf{t},\mathbf{t}\oplus\mathbf{r}) - H(\mathbf{r}) \\ &= nR + nh(p_e) - H(\mathbf{r}) \end{aligned} \tag{C.4}$$

We then divide $\mathbf{r}$ into two parts.

$$\mathbf{r} = \begin{pmatrix} \mathbf{r}_s & \mathbf{r}_c \end{pmatrix} \tag{C.5}$$

$\mathbf{r}_s$ is the first nR bits and $\mathbf{r}_c$ is the rest $n(1-R)$ bits. Let $r_c^{(i)}$ represent the ith bits of $\mathbf{r}_c$.

$H(\mathbf{r})$ can be expressed as

$$\begin{aligned} H(\mathbf{r}) = H(\mathbf{r}_c,\mathbf{r}_s) &= H(\mathbf{r}_c) + H(\mathbf{r}_c|\mathbf{r}_s) \\ &\leq nR + H(\mathbf{r}_c|\mathbf{r}_s) \\ &\leq nR + \sum_{i=1}^{n(1-R)} H(r_c^{(i)}|\mathbf{r}_s) \end{aligned}. \tag{C.6}$$

S. Xiao et al., *Dynamic Secrets in Communication Security*,
DOI: 10.1007/978-1-4614-7831-7,

The second $\leq$ is because the overlapping of parity check set can only reduce the uncertainty of $\mathbf{r}$.

Let $M^{(i)}$ represent the ith column in the random matrix M of M_G and M_H. $k(i)$ is the number of 1s in $M^{(i)}$.

$$\begin{aligned} H(r_c^{(i)}|\mathbf{r}_s) &= E_{\mathbf{r}_s \in \{0,1\}^{nR}}[H(r_c^{(i)}|\mathbf{r}_s)] \\ &= E_{\mathbf{r}_s \in \{0,1\}^{nR}}[h(p(r_c^{(i)} = \mathbf{r}_s M^{(i)}|\mathbf{r}_s))] \\ &= h(\phi_{k(i)+1}(p_e)) \\ &\leq h(\phi_{nR+1}(p_e)) \end{aligned} \tag{C.7}$$

The third equality is because M is a equiprobable random binary matrix, $p(r_c^{(i)} = \mathbf{r}_s M^{(i)}|\mathbf{r}_s)$ is the probability of even number of bit errors occur in this parity check set and this probability is unchanged for any $\mathbf{r}_s \in \{0, 1\}^{nR}$.

The last $\leq$ is because $h(\phi_k(p))$ is monotonically increasing with k and $k(i) \leq nR$.

Combining the Eqs. (C.4), (C.6) and (C.7) proves the theorem.

Theorem 6.3 *The probability of undetected errors is upper bounded by*

$$p_{ud} = p_{\mathbf{r} \in \Omega}(\mathbf{t} \neq \mathbf{r}) \leq \mathbf{2^{-n(1-R)}} \tag{C.8}$$

Proof Define the error vector $\mathbf{e}$ as

$$\mathbf{e} = \mathbf{t} \oplus \mathbf{r} = \begin{pmatrix} \mathbf{e}_s & \mathbf{e}_c \end{pmatrix}. \tag{C.9}$$

$\mathbf{e}_s$ contains the first nR bits of $\mathbf{e}$. $\mathbf{e}_c$ is the rest.

The syndrome of parity check $\mathbf{s}$ is

$$\mathbf{s} = \mathbf{e}M_H = \mathbf{e}_s M \oplus \mathbf{e}_c I_n(1 - R). \tag{C.10}$$

When $\mathbf{s} = 0$, the received vector $\mathbf{r}$ would be believed as no error-free. The event of undetected error occurs when $\mathbf{e} \neq \mathbf{0}$ and

$$\mathbf{e}_s M = \mathbf{e}_c. \tag{C.11}$$

There are three possible types of errors.

1. $\mathbf{e}_s = 0, \mathbf{e}_c \neq 0$
2. $\mathbf{e}_s \neq 0, \mathbf{e}_c = 0$
3. $\mathbf{e}_s \neq 0, \mathbf{e}_c \neq 0$

Type 1 errors will lead to non-zero syndrome and are always detected. Type 2 and 3 errors may escape the error detection. To analyze the probability of undetected errors, we expand Eq. (C.11) into an equation array.

$$\begin{cases} \mathbf{e}_s M^{(1)} & = e_c^{(1)} \\ & \vdots \\ \mathbf{e}_s M^{(i)} & = e_c^{(i)} \\ & \vdots \\ \mathbf{e}_s M^{(n(1-R))} & = e_c^{(n(1-R))} \end{cases} \tag{C.12}$$

M is an equiprobable random binary matrix. $M^{(i)}$ is a random binary string picked from $\{0, 1\}^{nR}$. Therefore no matter what the values of $\mathbf{e}_s$ and $e_c^{(i)}$ are, $p(\mathbf{e}_s M^{(i)} = e_c^{(i)}) = \frac{1}{2}$. Because each equation in the array (C.12) is independent to the others, the probability of all equations in (C.12) are satisfied would be $2^{-n(1-R)}$. Therefore we have

$$p_{ud} = p_{\mathbf{r}\in\Omega}(\mathbf{t} \neq \mathbf{r}) \leq 2^{-n(1-R)}. \tag{C.13}$$

The theorem is proved.

Appendix D
Reliability Analysis for Dynamic Key Based Two-Factor Authentication

D.1 MTTR and Average Availability

Recall the four state Markov model for dynamic key based two-factor authentication (Fig. D.1).

The mean time to recover is the expectation of time to stay in B state, which is the reciprocal of the exit rate of this state. Therefore, we have

$$MTTR_{two\text{-}key} = \frac{1}{\mu_c + \mu_m}. \tag{D.1}$$

The average availability is the probability that the system is not in B state in stationary phase. In order to find out the stationary distribution of this model, we first obtain the transition matrix $\mathbf{Q}$.

$$\mathbf{Q} = \begin{pmatrix} -(\lambda_m + \lambda_c) & \lambda_m & \lambda_c & 0 \\ \mu_m & -(\mu_m + \lambda_c) & 0 & \lambda_c \\ \mu_c & 0 & -(\mu_c + \lambda_m) & \lambda_m \\ 0 & \mu_c & \mu_m & -(\mu_c + \mu_m) \end{pmatrix} \tag{D.2}$$

The discrete time transition matrix $\mathbf{P}$ can be derived from $\mathbf{Q}$.

$$\mathbf{P} = \begin{pmatrix} 0 & \frac{\lambda_m}{\lambda_m + \lambda_c} & \frac{\lambda_c}{\lambda_m + \lambda_c} & 0 \\ \frac{\mu_m}{\mu_m + \lambda_c} & 0 & 0 & \frac{\lambda_c}{\mu_m + \lambda_c} \\ \frac{\mu_c}{\mu_c + \lambda_m} & 0 & 0 & \frac{\lambda_m}{\mu_c + \lambda_m} \\ 0 & \frac{\mu_c}{\mu_c + \mu_m} & \frac{\mu_m}{\mu_c + \mu_m} & 0 \end{pmatrix} \tag{D.3}$$

S. Xiao et al., *Dynamic Secrets in Communication Security*,
DOI: 10.1007/978-1-4614-7831-7,

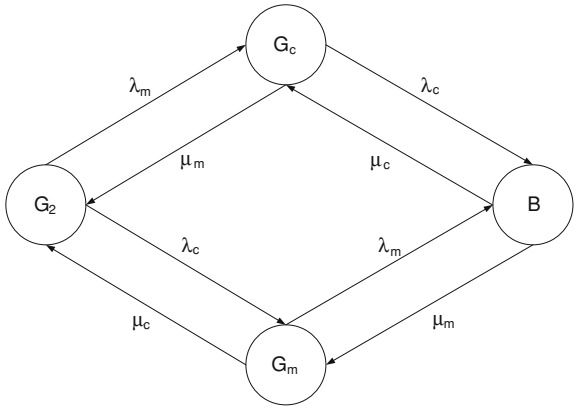

Fig. D.1 Four-state Markov model for dynamic key based two-factor authentication scheme. G_2 state means both keys are secret. G_c state means only the dynamic key on computer is secret. G_m state means only the dynamic key on mobile phone is secret. B state means both keys are known by adversary and the communication security is lost

The stationary distribution probability vector $\pi = [\pi_1, \pi_2, \pi_3, \pi_4]$ can be obtained from solving the equations

$$\begin{cases} \pi \mathbf{P} = \pi \\ \pi_1 + \pi_2 + \pi_3 + \pi_4 = 1 \end{cases}. \tag{D.4}$$

The average availability is

$$A_{avg,two\text{-}key} = 1 - \pi_4 = 1 - \frac{1}{2(1 + \frac{\mu_c \mu_m}{\mu_c + \mu_m} \frac{\lambda_c + \lambda_m}{\lambda_c \lambda_m})}. \tag{D.5}$$

D.2 MTFSF

The mean time to first system failure can be calculated from the model shown in Fig. D.2.

In the figure, B state is an absorbing state. We use T_{2B}, T_{cB}, and T_{mB} to denote the average time to reach the absorbing state from state G_2, G_c, and G_m respectively. T_{2B}, T_{cB}, and T_{mB} are related by the following equation array.

$$\begin{cases} T_{cB} = \frac{1}{\mu_m + \lambda_c} + \frac{\mu_m}{\mu_m + \lambda_c} T_{2B} \\ T_{mB} = \frac{1}{\mu_c + \lambda_m} + \frac{\mu_c}{\mu_c + \lambda_m} T_{2B} \\ T_{2B} = \frac{1}{\lambda_c + \lambda_m} + \frac{\lambda_m}{\lambda_c + \lambda_m} T_{cB} + \frac{\lambda_c}{\lambda_c + \lambda_m} T_{mB} \end{cases} \tag{D.6}$$

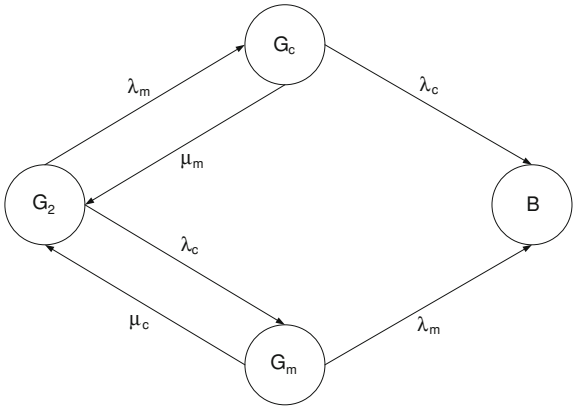

Fig. D.2 Four-state Markov model to calculate MTFSF for dynamic key based two-factor authentication scheme. G_2 state means both keys are secret. G_c state means only the dynamic key on computer is secret. G_m state means only the dynamic key on mobile phone is secret. B state means both keys are known by adversary and the communication security is lost

The MTFSF of the authentication scheme can be found by solving the above equation array. We have

$$MTFSF_{two\text{-}key} = T_{2B} = \frac{1 + \frac{\lambda_m}{\mu_m + \lambda_c} + \frac{\lambda_c}{\mu_c + \lambda_m}}{\lambda_c \lambda_m (\frac{1}{\mu_m + \lambda_c} + \frac{1}{\mu_c + \lambda_m})}. \tag{D.7}$$

References

1. Adams, C., Lloyd, S.: Understanding PKI: Concepts, Standards, and Deployment Considerations, 2nd edn. Addison-Wesley Longman Publishing, Boston (2002)
2. Al-Bakri, S., Kiah, M., Zaidan, A., Zaidan, B., Alam, G.: Securing peer-to-peer mobile communications using public key cryptography: new security strategy. Int. J. Phys. Sci. **6**(4), 930–938 (2011)
3. Al-Janabi, S., Rasheed, M.S.: Public-key cryptography enabled kerberos authentication. In: Developments in E-systems Engineering (DeSE), 2011, pp. 209–214 (2011)
4. Amin, M.: Challenges in reliability, security, efficiency, and resilience of energy infrastructure: toward smart self-healing electric power grid. In: Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, pp. 1–5 (2008)
5. Anderson, R.J. (ed.): Fast Software Encryption, Cambridge Security Workshop, Cambridge, UK, December 9–11, 1993, Proceedings. Lecture Notes in Computer Science, vol. 809. Springer (1994)
6. Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C., Vittal, V.: Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. IEEE Trans. Power Syst. **20**(4), 1922–1928 (2005)
7. Andgren, M., Hell, M., Johansson, T.: On hardware-oriented message authentication with applications towards RFID. In: Lightweight Security Privacy: Devices, Protocols and Applications (LightSec), 2011 Workshop on, pp. 26–33 (2011)
8. Aono, T., Higuchi, K., Ohira, T., Komiyama, B., Sasaoka, H.: Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. IEEE Trans. Antenn. Prop. **53**(11), 3776–3784 (2005)
9. Arfman, J.M., Roden, P.: Project Athena: supporting distributed computing at MIT. IBM Syst. J. **31**(3), 550–563 (1992)
10. Azimi-Sadjadi, B., Kiayias, A., Mercado, A., Yener, B.: Robust key generation from signal envelopes in wireless networks. In: CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 401–410. ACM, New York, NY, USA (2007)
11. Bardou, R., Focardi, R., Kawamoto, Y., Simionato, L., Steel, G., Tsay, J.K.: Efficient padding oracle attacks on cryptographic hardware. In: Safavi-Naini, R., Canetti, R. (eds.) Advances in Cryptology, CRYPTO 2012. Lecture Notes in Computer Science, vol. 7417, pp. 608–625. Springer, Berlin (2012)

S. Xiao et al., *Dynamic Secrets in Communication Security*,
DOI: 10.1007/978-1-4614-7831-7,

12. Barker, W.C.: Recommendation for the triple data encryption algorithm (TDEA) block cipher. Technical Report, NIST (2008)
13. Barlow, R., Proschan, F., Hunter, L.: Mathematical theory of reliability. Classics in applied mathematics. SIAM (1996)
14. Barros, J., Rodrigues, M.R.D.: Secrecy capacity of wireless channels. Information Theory, 2006 IEEE International Symposium on, pp. 356–360 (2006)
15. Bauer, M., Plappert, W., Wang, C., Dostert, K.: Packet-oriented communication protocols for smart grid services over low-speed PLC. In: Power Line Communications and Its Applications, 2009. ISPLC 2009. IEEE International Symposium on, pp. 89–94 (2009)
16. Baumeister, T.: Adapting PKI for the smart grid. In: Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, pp. 249–254 (2011)
17. Bell, J.: Mars exploration: roving the red planet. Nature **490**(7418), 34–35 (2012)
18. Bello, L.: DSA-1571-1 openssl—predictable random number generator. Tech. rep., www.Debian.org (2008)
19. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. J. Cryptol. **5**, 3–28 (1992)
20. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE Press, New York (1984)
21. Bennett, C.H., Brassard, G., Crkpeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theory **41**, 1915–1923 (1995)
22. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2), 210–229 (1988)
23. Bittau, A., Handley, M., Lackey, J.: The final nail in WEP's coffin. In: Security and Privacy, 2006 IEEE Symposium on, pp. 15–400. doi:10.1109/SP.2006.40 (2006)
24. Bloch, M., Barros, J., Rodrigues, M.R.D., McLaughlin, S.W.: Wireless information-theoretic security, Theoretical aspects. IEEE Trans. Inf. Theory, **54**(6), 2515–2534 (2008)
25. Carter, J.L., Wegman, M.N.: Universal classes of hash functions (extended abstract). In: Proceedings of the Ninth Annual ACM Symposium on Theory of Computing, STOC '77, pp. 106–112. ACM, New York, NY, USA (1977)
26. Carter, J.L., Wegman, M.N.: Universal classes of hash functions. J. Comput. Syst. Sci. **18**, 396–407 (1979)
27. de Carvalho, J., Veiga, H., Gomes, P., Pacheco, C., Marques, N., Reis, A.: Laboratory performance of wi-fi point-to-point links: a case study. In: Wireless Telecommunications Symposium, 2009. WTS 2009, pp. 1–5 (2009)
28. Chevassut, O., Alain Fouque, P., Gaudry, P., Pointcheval, D.: Key derivation and randomness extraction. In: Proceedings of Crypto'05 (2005)
29. Chong, Z., Jorswieck, E.: Energy efficiency in random opportunistic beamforming. In: Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd, pp. 1–5 (2011)
30. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley-Interscience, New York (1991)
31. Cronin, E., Sherr, M., Blaze, M.: On the (un)reliability of eavesdropping. Int. J. Secur. Netw. (IJSN) **3**(2), 103–113 (2008)
32. Deconinck, G.: An evaluation of two-way communication means for advanced metering in flanders (Belgium). In: Instrumentation and Measurement Technology Conference Proceedings, 2008. IMTC 2008. IEEE, pp. 900–905 (2008)
33. Delsing, J., Eliasson, J., Leijon, V.: Latency and packet loss of an interferred 802.15.4 channel in an industrial environment. In: Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on, pp. 33–38 (2010)
34. Ding, Z., Leung, K., Goeckel, D., Towsley, D.: On the application of cooperative transmission to secrecy communications. IEEE J. Sel. Areas Commun. **30**(2), 359–368 (2012)
35. Dorrendorf, L., Gutterman, Z., Pinkas, B.: Cryptanalysis of the random number generator of the windows operating system. ACM Trans. Inf. Syst. Secur. **13**(1), 10:1–10:32 (2009)

36. Dutta, P., Dawson-Haggerty, S., Chen, Y., Liang, C.J.M., Terzis, A.: Design and evaluation of a versatile and efficient receiver-initiated link layer for low-power wireless. In: Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems, SenSys '10, pp. 1–14. ACM, New York, NY, USA (2010)
37. Finke, T., Gebhardt, M., Schindler, W.: A new side-channel attack on RSA prime generation. In: Clavier, C., Gaj, K. (eds.) Cryptographic Hardware and Embedded Systems—CHES 2009. Lecture Notes in Computer Science, vol. 5747, pp. 141–155. Springer, Berlin (2009)
38. Flatraaker, D.I.: Mobile, internet and electronic payments: the key to unlocking the full potential of the internal payments market. J. Paym. Strategy Syst. **3**(1), 60–70 (2009)
39. Florencio, D., Herley, C.: A large-scale study of web password habits. In: WWW '07: Proceedings of the 16th international Conference on World Wide Web, pp. 657–666. ACM, New York, NY, USA (2007)
40. Floyd, S., Fall, K.: Promoting the use of end-to-end congestion control in the internet. IEEE/ACM Trans. Netw. **7**(4), 458–472 (1999)
41. Frst, M., Weier, H., Nauerth, S., Marangon, D.G., Kurtsiefer, C., Weinfurter, H.: High speed optical quantum random number generation. Optics Express **18**, 13,029–13,037 (2010)
42. Furnell, S., Clarke, N., Karatzouni, S.: Beyond the pin: enhancing user authentication for mobile devices. Comput. Fraud Secur. **2008**(8), 12–17 (2008)
43. Gafurov, D., Snekkenes, E., Buvarp, T.: Robustness of biometric gait authentication against impersonation attack. In: Meersman, R., Tari, Z., Herrero, P. (eds.) On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops. Lecture Notes in Computer Science, vol. 4277, pp. 479–488. Springer, Berlin (2006)
44. Goeckel, D., Vasudevan, S., Towsley, D., Adams, S., Ding, Z., Leung, K.: Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks. IEEE J. Sel. Areas Commun. **29**(10), 2067–2076 (2011)
45. Gollmann, D. (ed.): Fast Software Encryption, Third International Workshop, Cambridge, UK, 21–23 February 1996, Proceedings. Lecture Notes in Computer Science, vol. 1039. Springer, Berlin (1996)
46. Guneysu, T., Kasper, T., Novotny, M., Paar, C., Rupp, A.: Cryptanalysis with COPACOBANA. IEEE Trans. Comput. **57**(11), 1498–1513 (2008)
47. Hassan, A.A., Stark, W.E., Hershey, J.E.: Cryptographic key agreement for mobile radio. Dig. Sig. Process. **6**, 207–212 (1996)
48. Heinzelman, W. R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on, vol. 2, p. 10 (2000)
49. Herley, C.: So long, and no thanks for the externalities: the rational rejection of security advice by users. In: NSPW '09: Proceedings of the 2009 Workshop on New Security Paradigms Workshop, pp. 133–144. ACM, New York, NY, USA (2009)
50. Honan, M.: How apple and amazon security flaws led to my epic hacking
51. IEEE: IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements—Part 11: Wireless LAN medium access control (MAC) and physical layer (phy) specifications. IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999) pp. C1–1184 (2007)
52. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Commun. ACM **50**(10), 94–100 (2007)
53. Jana, S., Premnath, S.N., Clark, M., Kasera, S.K., Patwari, N., Krishnamurthy, S.V.: On the effectiveness of secret key extraction from wireless signal strength in real environments. In: Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, MobiCom '09, pp. 321–332. ACM, New York, NY, USA (2009)
54. Janssen, J., De Vleeschauwer, D., Buchli, M., Petit, G.: Assessing voice quality in packet-based telephony. IEEE Internet Comput. **6**(3), 48–56 (2002)
55. Jonsson, E., Olovsson, T.: An empirical model of the security intrusion process. In: Computer Assurance, 1996. COMPASS '96, 'Systems Integrity, Software Safety, and Process Security'. Proceedings of the Eleventh Annual Conference on, pp. 176–186 (1996)

56. Jonsson, E., Olovsson, T.: A quantitative model of the security intrusion process based on attacker behavior. IEEE Trans. Softw. Eng. **23**(4), 235–245 (1997)
57. Kentros, S., Albayram, Y., Bamis, A.: Towards macroscopic human behavior based authentication for mobile transactions. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing, pp. 641–642. ACM (2012)
58. Kerckhoffs, A.: La cryptographie militaire. J. Sci. Militaires **IX**, 5–83 (1883)
59. Key, P., Massoulié, L., Towsley, D.: Path selection and multipath congestion control. Commun. ACM **54**(1), 109–116 (2011)
60. Han H, Srinivas S, C. V. Hollot, R. Srikant, and Donald Towsley. Multi-path TCP: a joint congestion control and routing scheme to exploit path diversity in the internet. IEEE/ACM Trans. Netw. 14(6), 1260–1271 (2006)
61. Khurana, H., Hadley, M., Lu, N., Frincke, D.: Smart-grid security issues. IEEE Secur. Priv. **8**(1), 81–85 (2010)
62. Kinney, R., Crucitti, P., Albert, R., Latora, V.: Modeling cascading failures in the North American power grid. Eur. Phys. J. B: Condens. Matter Complex Syst. **46**, 101–107 (2005)
63. Klein, A.: Attacks on the RC4 stream cipher. Des. Codes Crypt. **48**, 269–286 (2008)
64. Koch, R., Stelte, B., Golling, M.: Attack trends in present computer networks. In: Cyber Conflict (CYCON), 2012 4th International Conference on, pp. 1–12 (2012)
65. Korhonen, J., Wang, Y.: Effect of packet size on loss rate and delay in wireless links. In: Wireless Communications and Networking Conference, 2005 IEEE, vol. 3, pp. 1608–1613 (2005)
66. Kouyoumdjieva, S., Helgason, l., Yavuz, E.A., Karlsson, G.: Evaluating an energy-efficient radio architecture for opportunistic communication. In: Proceedings of 3rd Workshop on Energy Efficiency in Wireless Networks and Wireless Networks for Energy Efficiency (E2Nets) (2012). QC 20120803
67. Krawczyk, H.: LFSR-based hashing and authentication. In: Desmedt, Y. (ed.) Advances in Cryptology. CRYPTO 94. Lecture Notes in Computer Science, vol. 839, pp. 129–139. Springer, Berlin (1994)
68. Kurita, S., Komoriya, K., Uda, R.: Privacy protection on transfer system of automated teller machine from brute force attack. In: Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, pp. 72–77 (2012)
69. Laptyeva, T.V., Flach, S., Kladko, K.: The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs. Cryptology ePrint Archive, Report 2011/172 (2011)
70. Latif, M.A., Sultan, A., Gamal, H.E.: ARQ-based secret key sharing. In: ICC, pp. 1–6 (2009)
71. Latif, M.A., Sultan, A., Gamal, H.E.: ARQ secrecy over correlated fading channels. In: Information Theory Workshop, 2010. ITW 2010. IEEE (2010)
72. Lefebvre, S., Porteous, H.: The Russian 10.. 11: an inconsequential adventure? Int. J. Intell. Counter Intell. **24**(3), 447–466 (2011)
73. Li, C., Li, H., Kohno, R.: Performance evaluation of IEEE 802.15. 4 for wireless body area network (WBAN). In: Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on, pp. 1–5. IEEE (2009)
74. Li, H., Han, Z., Lai, L., Qiu, R., Yang, D.: Efficient and reliable multiple access for advanced metering in future smart grid. In: Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, pp. 440–444 (2011)
75. Li, Y., Xiong, Y., Yang, S.: Study on mobile commerce authentication system. In: Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, pp. 1–4 (2011)
76. Liu, R., Liu, T., Poor, H.V., Shamai, S.: Multiple-input multiple-output Gaussian broadcast channels with confidential messages. CoRR **abs/0903.3786** (2009)
77. Liu, R., Poor, H.: Multi-antenna Gaussian broadcast channels with confidential messages. In: ISIT 2008. IEEE International Symposium on Information Theory, 2008 (2008)
78. Lobato, R., Thomas, J.: The business of anti-piracy: new zones of enterprise in the copyright wars. Int. J. Commun. **5** (2011)

79. Long, H., Liu, Y., Fan, X., Dick, R.P., Yang, H.: Energy-efficient spatially-adaptive clustering and routing in wireless sensor networks. In: Proceedings of the Conference on Design, Automation and Test in Europe, DATE '09, pp. 1267–1272. European Design and Automation Association, 3001 Leuven, Belgium, Belgium (2009)
80. Lumezanu, C., Guo, K., Spring, N., Bhattacharjee, B.: The effect of packet loss on redundancy elimination in cellular wireless networks. In: Proceedings of the 10th Annual Conference on Internet Measurement, IMC '10, pp. 294–300. ACM, New York, NY, USA (2010)
81. Main, A., van Oorschot, P.: Software protection and application security: understanding the battleground. International Course on State of the Art and Evolution of Computer Security and Industrial Cryptography, Heverlee, Belgium (2003)
82. Mathur, S., Trappe, W., Mandayam, N., Ye, C., Reznik, A.: Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In: MobiCom '08: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, pp. 128–139. ACM, New York, NY, USA (2008)
83. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**, 733–742 (1993)
84. Maurer, U.M., Wolf, S.: Secret key agreement over a non-authenticated channel—Part I: Definitions and bounds. IEEE Trans. Inf. Theory **49**, 822–831 (2003)
85. Maurer, U.M., Wolf, S.: Secret key agreement over a non-authenticated channel—Part II: The simulatability condition. IEEE Trans. Inf. Theory **49**, 832–838 (2003)
86. Maurer, U.M., Wolf, S.: Secret key agreement over a non-authenticated channel—Part III: Privacy amplification. IEEE Trans. Inf. Theory **49**, 839–851 (2003)
87. Melia-Segui, J., Garcia-Alfaro, J., Herrera-Joancomarti, J.: Analysis and improvement of a pseudorandom number generator for EPC Gen2 tags. In: Sion, R., Curtmola, R., Dietrich, S., Kiayias, A., Miret, J., Sako, K., Seb, F. (eds.) Financial Cryptography and Data Security. Lecture Notes in Computer Science, vol. 6054, pp. 34–46. Springer, Berlin (2010)
88. Miao, G., Himayat, N., Li, Y.G., Swami, A.: Cross-layer optimization for energy-efficient wireless communications: a survey. Wireless Commun. Mobile Comput. **9**(4), 529–542 (2009)
89. Miller, F., Vandome, A., McBrewster, J.: Key-Agreement Protocol. VDM Verlag Dr. Mueller e.K. (2010)
90. Naumovich, G., Memon, N.: Preventing piracy, reverse engineering, and tampering. Computer **36**(7), 64–71 (2003)
91. NIST: Federal information processing standards publication 197. Technical Report, NIST (2001)
92. Omar, Y., Youssef, M., El Gamal, H.: ARQ secrecy: from theory to practice. In: Information Theory Workshop, 2009. ITW 2009. IEEE, pp. 6–10 (2009)
93. Pareschi, F., Scotti, G., Giancane, L., Rovatti, R., Setti, G., Trifiletti, A.: Power analysis of a chaos-based random number generator for cryptographic security. In: Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on, pp. 2858–2861 (2009)
94. Paxson, V.: End-to-end routing behavior in the internet. SIGCOMM Comput. Commun. Rev. **26**(4), 25–38 (1996)
95. Pièrre-Cambacédès, L., Sitbon, P.: Cryptographic key management for SCADA systems-issues and perspectives. In: Proceedings of the 2008 International Conference on Information Security and Assurance (ISA 2008), ISA '08, pp. 156–161. IEEE Computer Society, Washington, DC, USA (2008)
96. Piller, C.: How piracy opens doors for windows. Los Angeles Times **9** (2006)
97. Podhoransky, P., Lipovsky, M., Zemanovic, J., Sabo, M.: Transfer and error rate measurement in the Lon works power line communication systems. In: Radioelektronika, 2007. 17th International Conference, pp. 1–3 (2007)
98. Power, R., Forte, D.: Social engineering: attacks have evolved, but countermeasures have not. Comput. Fraud Secur. **2006**(10), 17–20 (2006)
99. Raghuvamshi, A., Rao, P.: An effortless cryptanalytic attack on knapsack cipher. In: Process Automation, Control and Computing (PACC), 2011 International Conference on, pp. 1–6 (2011)

100. Rana, M., Ahmed, K., Sumel, N., Alam, M., Sarkar, L.: Security in ad hoc networks: a location based impersonation detection method. In: Computer Engineering and Technology, 2009. ICCET '09. International Conference on, vol. 2, pp. 380–384 (2009)
101. Rappaport, T.: Wireless Communications: Principles and Practice. Prentice Hall PTR, Upper Saddle River (2001)
102. Ren, Y., Xing, T., Cao, G., Xu, E., Chen, X.: Research and practice on the cooperative concealing technology of trojan horses. In: Networking and Digital Society (ICNDS), 2010 2nd International Conference on, vol. 1, pp. 216–219 (2010)
103. Renyi, A.: On measures of information and entropy. In: Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability (1960)
104. Rivest, R.L.: The RC4 Encryption Algorithm. RSA Data Security, Inc. (1992)
105. Romero-Jerez, J., Goldsmith, A.: Receive antenna array strategies in fading and interference: an outage probability comparison. IEEE Trans. Wireless Commun. **7**(3), 920–932 (2008)
106. Romirer-Maierhofer, P., Ricciato, F., D'Alconzo, A., Franzan, R., Karner, W.: Network-wide measurements of TCP RTT in 3G. In: TMA, pp. 17–25 (2009)
107. Rozema, L., Darabi, A., Mahler, D., Hayat, A., Soudagar, Y., Steinberg, A.M.: Direct violation of Heisenberg's precision limit by weak measurements. In: Frontiers in Optics Conference, p. FW4J.4. Optical Society of America (2012)
108. Salem, M., Stolfo, S.: Modeling user search behavior for masquerade detection. In: Sommer, R., Balzarotti, D., Maier, G. (eds.) Recent Advances in Intrusion Detection. Lecture Notes in Computer Science, vol. 6961, pp. 181–200. Springer, Berlin (2011)
109. Sathish Babu, B., Venkataram, P.: A dynamic authentication scheme for mobile transactions. Int. J. Netw. Secur. **8**(1), 59–74 (2009)
110. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, New York (1995)
111. Serrano, P., Zink, M., Kurose, J.: Assessing the fidelity of cots 802.11 sniffers. In: INFOCOM 2009, IEEE, pp. 1089–1097 (2009)
112. Shafiq, M.Z., Ji, L., Liu, A.X., Pang, J., Wang, J.: A first look at cellular machine-to-machine traffic: large scale measurement and characterization. SIGMETRICS Perform. Eval. Rev. **40**(1), 65–76 (2012)
113. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)
114. Sheth, A., Nedevschi, S., Patra, R., Surana, S., Brewer, E., Subramanian, L.: Packet loss characterization in wifi-based long distance networks. In: INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, pp. 312–320 (2007)
115. Siam, M., Krunz, M., Cui, S., Muqattash, A.: Energy-efficient protocols for wireless networks with adaptive MIMO capabilities. Wireless Netw. **16**, 199–212 (2010)
116. Sieka, B.: Using radio device fingerprinting for the detection of impersonation and Sybil attacks in wireless networks. In: Buttyn, L., Gligor, V., Westhoff, D. (eds.) Security and Privacy in Ad-Hoc and Sensor Networks. Lecture Notes in Computer Science, vol. 4357, pp. 179–192. Springer, Berlin (2006)
117. Singh, S.: The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography, 1st edn. Doubleday, New York (1999)
118. Smith, S.: Cryptographic scalability challenges in the smart grid (extended abstract). In: Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES, pp. 1–3 (2012)
119. Stevens, R.W.: Unix Network Programming. Prentice Hall PTR, Upper Saddle River (1990)
120. Tanenbaum, A.: Computer networks. Prentice Hall PTR, Upper Saddle River (2003)
121. Tang, X., Liu, R., Spasojevic, P., Poor, H.: On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels. IEEE Trans. Inf. Theory **55**(4), 1575–1591 (2009)
122. Tao, Z., Nath, B., Lonie, A.: A data clustering approach to discriminating impersonating devices in wi-fi networks. Secur. Commun. Netw. **3**(1), 44–57 (2010)
123. Thornburgh, T.: Social engineering: the "dark art". In: Proceedings of the 1st Annual Conference on Information Security Curriculum Development, InfoSecCD '04, pp. 133–135. ACM, New York, NY, USA (2004)

124. Viega, J.: Practical random number generation in software. In: Computer Security Applications Conference, 2003. Proceedings. 19th Annual, pp. 129–140 (2003)
125. Vishnani, K., Pais, A.R., Mohandas, R.: An in-depth analysis of the epitome of online stealth: keyloggers; and their countermeasures. In: Abraham, A., Mauri, J.L., Buford, J.F., Suzuki, J., Thampi, S.M. (eds.) Advances in Computing and Communications. Communications in Computer and Information Science, vol. 192, pp. 10–19. Springer, Berlin (2011)
126. Weir, M., Aggarwal, S., Collins, M., Stern, H.: Testing metrics for password creation policies by attacking large sets of revealed passwords. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10, pp. 162–175. ACM, New York, NY, USA (2010)
127. Wilson, R., Tse, D., Scholtz, R.: Channel identification: secret sharing using reciprocity in ultrawideband channels. In: ICUWB 2007, pp. 270–275 (2007)
128. Wong, C.W., Shea, J., Wong, T.: Secret sharing in fast fading channels based on reliability-based hybrid ARQ. In: MILCOM 2008. IEEE, pp. 1–7 (2008)
129. Xiao, S., Pishro-Nik, H., Gong, W.: Dense parity check based secrecy sharing in wireless communications. In: Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE, pp. 54–58 (2007)
130. Yang, C., Hung, J.L., Lin, Z.X.: Loose password security in chinese cyber world left the front door wide open to hackers: an analytic view. In: Proceedings of the 14th Annual International Conference on Electronic Commerce, ICEC '12, pp. 121–126. ACM, New York, NY, USA (2012)
131. Yang, D., Sonmez, M., Bosworth, D., Fryxell, G.: Global software piracy: searching for further explanations. J. Bus. Ethics **87**(2), 269–283 (2009)
132. Yin, J., Ren, J.G., Lu, H., Cao, Y., Yong, H.L., Wu, Y.P., Liu, C., Liao, S.K., Zhou, F., Jiang, Y.: Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. Nature **488**(7410), 185188 (2012). http://www.nature.com/nature/journal/v488/n7410/abs/nature11332.html
133. Yurcik, W., Liu, C.: A first step toward detecting SSH identity theft in HPC cluster environments: discriminating masqueraders based on command behavior. In: Cluster Computing and the Grid, 2005. CCGrid 2005. IEEE International Symposium on, vol. 1, pp. 111–120 (2005)
134. Zeng, K., Govindan, K., Wu, D., Mohapatra, P.: Identity-based attack detection in mobile wireless networks. In: INFOCOM, 2011 Proceedings IEEE, pp. 1880–1888 (2011)
135. Zhao, S., Shoniregun, C.: Critical review of unsecured WEP. In: Services, 2007 IEEE Congress on, pp. 368–374 (2007)
136. Zhu, W., Thomborson, C., Wang, F.: A survey of software watermarking. Intelligence and Security Informatics, pp. 283–331 (2005)

Index

S. Xiao et al., *Dynamic Secrets in Communication Security*,
DOI: 10.1007/978-1-4614-7831-7,